Information and Intelligence Sharing in the Fight Against Fraud and Intellectual Property Crime: Challenges and Strategies for Professional Practice

Carl Watson

The thesis is submitted in partial fulfilment of the requirements for the award of the degree of Doctor of Criminal Justice of the University of Portsmouth.

25 October 2017

Declaration

Whilst registered as a candidate for the above degree, I have not been registered for any other research award. The results and conclusions embodied in this thesis are the work of the named candidate and have not been submitted for any other academic award.

Word count: 51,292

Acknowledgements

I could not have conducted and completed this work over the past few years without the help and support of many people. First and foremost, I wish to thank my wife Jo, and stepsons Conor and Luke, for their support and understanding over the years, and I am also grateful to other family and friends for sticking by me through it. I am also grateful for the encouragement and advice given by my supervisory team, Professor Mark Button and Dr Alison Wakefield.

I am deeply indebted to Kieron Sharp at the Federation Against Copyright Theft for being so open to taking part in the study, and to the officers and staff of that organisation. Likewise, I am grateful to all of the interviewees from other organisations who consented to take part in the research. I must also acknowledge and thank Tim Harvey of the ACFE UK for his endless interest, encouragement and willingness to for me to exploit his extensive contact list, as well as Roy Burnett and Steve Hyndman for providing additional useful contacts. Finally I would like to express deep gratitude to my former manager, Mark Kinsella, for his support and enthusiasm.

I would like to dedicate this thesis to the memory of Matt Atwell, one of my closest friends, who suddenly and unexpectedly passed away whilst I was conducting the research. You are sadly missed and will always be remembered.

Table of Contents

List of Figures

List of Abbreviations

3x5x2 – UK intelligence grading system (revised from previous 5x5x5 grading system). Can also refer to a UK Intelligence Report

5x5x5 – UK intelligence grading system. Can also refer to a UK Intelligence Report

9/11 Commission – National Commission on Terrorist Attacks Upon the United States

ACFE – Association of Certified Fraud Examiners

ACPO – Association of Chief Police Officers

BCU – Basic Command Unit [police]

Brexit – British exit from the European Union

CHIS – Covert Human Intelligence Sources

CICJIS – Colorado Integrated Criminal Justice Information System

CIFAS – Credit Industry Fraud Avoidance System

CMS – Case Management System

COLP – City of London Police

DCMA – Digital Millennium Copyright Act [US]

DELJIS – Delaware Justice Information System

DPA – Data Protection Act 1998

DVD – Digital Versatile Disc

DVLA – Driver & Vehicle Licensing Agency

DWP – Department for Work & Pensions

FACT – Federation Against Copyright Theft

FAP – Fraud Advisory Panel

GAIN – Government Agency Intelligence Network

GDP – Gross Domestic Product

GDPR – EU General Data Protection Regulation

HMIC – Her Majesty's Inspectorate of Constabulary

HMRC – Her Majesty's Revenue & Customs

ICO – Information Commissioners' Office

IFB – Insurance Fraud Bureau

IFED – Insurance Fraud Enforcement Department

ILP – Intelligence-Led Policing

IPP – Intelligence Professionalisation Programme

IMS – Intelligence Management System

IP Crime – Intellectual Property Crime

IPO – Intellectual Property Office

IPS – Identity & Passport Service

JNET – Commonwealth of Pennsylvania Justice Network

MPA – Motion Picture Association [of America, also known as MPAA]

MOPI – Management of Police Information

MOU – Memorandum of Understanding

NAO – National Audit Office

NCA – National Crime Agency

NCIS – National Criminal Intelligence Service

NFA – National Fraud Authority

NFSA – National Fraud Strategic Authority

NFI – National Fraud Initiative

NFIB – National Fraud Intelligence Bureau

NIM – National Intelligence Model

NOMS – National Offender Management Service

OECD – Organisation for Economic Co-operation and Development

ONS – Office for National Statistics

PCSO – Police Community Support Officer

PIU – Performance and Innovation Unit [Cabinet Office]

RIPA – Regulation of Investigatory Powers Act 2000

SAFO – Specified Anti-Fraud Organisation

SCA – Serious Crime Act 2007

SEC – U.S. Securities and Exchange Commission

SLA – Service Level Agreement

SOCA – Serious Organised Crime Agency

SFO – Serious Fraud Office

SPOC – Single Point of Contact

Glossary of Key Terms

5x5x5

A 5x5x5 intelligence report is an applied methodology for the evaluation and dissemination of incoming and outgoing intelligence. The numbers reference a tripartite system to evaluate data and control dissemination, using a five-point scale to grade the trustworthiness of the source, the reliability of the information or intelligence described on the report and to assign a handling code to indicate how widely the intelligence may be disseminated. The model has recently been superseded by an alternative system, the 3x5x2 which was designed to be more straightforward, especially with respect to dissemination.

Chatham House Rule

The Chatham House Rule is a widely recognised and observed protocol that is used to enable the presentation or discussion of potentially sensitive information in a forum that may comprise representatives of many and diverse organisations. The convention stipulates that while participants may subsequently use or refer to the information disclosed during the meeting, they may not reveal the identity of the speaker or other participants. The Rule was devised in 1927 by The Royal Institute of International Affairs, and was most recently refined in 2002. While it can be common for meetings using the convention to refer to *Chatham House Rules*, there is only one such Rule in place. The formal wording of the Rule is:

> *"When a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed."* (Chatham House, 2017).

Government Agency Intelligence Network (GAIN)

GAIN networks are multi-organisational, cross-sector information and intelligence sharing networks that operate across the UK, organised primarily on a regional basis although with some local GAINs operating at more localised (e.g. city) levels. GAINs are based within police Regional Organised Crime Units [ROCUs]. The networks are organised around a central GAIN Coordinator who acts as the central conduit for intelligence sharing, managing requests and referrals from partner agencies in a hub-and-spoke model. The networks allow both the coordination of action amongst

partner agencies against criminal targets and as a means of allowing organisations to request intelligence searches of other members' intelligence databases. GAINs can include amongst their membership organisations that operate across all sectors.

Intelligence-Led Policing (ILP)

Intelligence-Led Policing is a model of policing that focuses on the use of intelligence to determine the priorities for allocation of policing resource according to risk. It was developed as a proactive approach to policing targeting patterns of problem areas and prolific offenders, rather than the reactive models that preceded it which focussed on the response to individual incidents.

Management of Police Information (MOPI)

MOPI is a framework for the collection, handling, storage, retention, review, destruction and sharing of information collected by police forces in England and Wales. The principles and responsibilities for MOPI are set out in a Code of Practice issued in 1995 by the Home Office, under the Police Act 1996 and the Police Act 1997. The code sets out principles of practice for the handling of data – including personal data, information and intelligence – collected for policing purposes, and the responsibilities incumbent upon Chief Constables to put into place systems and procedures to ensure compliance with the code.

Memorandum of Understanding (MOU)

A Memorandum of Understanding, or an Information Sharing Agreement, is a formal written agreement between two parties that can be used to establish the basis on which an information-sharing relationship is based. These take many different forms, but can include details such as the purpose of the agreement, the circumstances for sharing, the legal basis under which information sharing will take place, key parties and points of contact, and the process by which information sharing will take place. It may also formalise the rights and obligations of the parties, and any mechanisms to check and review that the processes, and agreement, are functioning as intended.

National Fraud Initiative (NFI)

The National Fraud Initiative, initially set up in 1996, is a multi-agency and cross sector data matching project run by the Cabinet Office (and previously by the Audit Commission). The project operates on a biennial cycle, collecting payroll and creditor data from participating organisations from the public, private and not-for-profit sectors. This data is matched across all participating agencies and relevant matches

that may indicate potential fraud is returned to each organisation for review and, where appropriate, investigation. The NFI is credited with helping participating organisations identify £1.39 billion of fraud and overpayments since its inception.

National Intelligence Model (NIM)

The National Intelligence Model is a business model designed for law enforcement around the concept of Intelligence-Led Policing. The model was developed by the UK's National Criminal Intelligence Service and implemented across UK police forces in the early 2000s. It defines a process for intelligence-led policing decisions operating at three levels: local, cross-border and organised crime. The model outlines central processes including Tasking and Coordination Groups which meet to determine policing priorities and allocate resources based on a defined set of products that assist in this decision making. These products are split into four categories: analytical products, intelligence products, knowledge products and system products.

Specified Anti-Fraud Organisation (SAFO)

Sections 68-72 of the Serious Crime Act 2007 provides a legal gateway for public sector authorities to share sensitive information and intelligence with organisations designated under the legislation as Specified Anti-Fraud Organisations for the purposes of the prevention, detection and investigation of fraud. This gateway may be used so long as the disclosure does not breach the Data Protection Act 1998 or any obligation of confidence that the authority has, and that the disclosure is not prohibited by Part 1 of the Regulation of Investigatory Powers Act 2000 [RIPA]. This gateway was designed to facilitate appropriate cross-sector sharing from the public sector to private and not-for-profit sector organisations. The Serious Crime Act 2007 required the government to produce a code of practice for sharing under the provision. SAFO status is conferred upon organisations whose purpose and procedures have been vetted and approved as being competent in handling and processing such data for the purposes of combating fraud.

Single Point of Contact (SPOC)

A Single Point of Contact is a party within an organisation designated as the formal contact or gatekeeper within an information sharing relationship, and the point through which requests for information or intelligence would normally be channelled. They will commonly also be the point from which information and intelligence will be disseminated under the same relationship. In many cases, the SPOC will be

identified for each party within a formal MOU document. While often the SPOC will be a single person or contact point within an organisation or department, given the size of many organisations (such as multinational corporations) there may be more than one designated SPOC. SPOCs will often also act both as gatekeeper and as arbiters or guarantors of the quality and reliability of shared information and of the rules under which it is disseminated.

Abstract

Information and intelligence sharing has long been recognised to be a practice that could have significant bearing on organisations' ability to prevent, detect, investigate and take action against economic crime. Despite this recognition, many businesses struggle to build and maintain effective information sharing relationships. This research aims to close the gap caused by limited academic attention paid to economic crime information sharing, examining the contemporary nature of the challenges, the models and strategies that can be used to overcome these and how professional practice can be improved to increase information and intelligence sharing in this area.

Data was collected in two phases in order to examine how those organisations that manage to successfully share information and intelligence overcome the challenges to collaboration. The first phase involved a case study into how the Federation Against Copyright Theft handles and shares intelligence with partners. This involved twenty-four interviews with officers and staff and examining documents relating to its operational activity and on-site observations. The second phase of the research involved conducting twenty-two interviews with participants from other organisations in respect of their approaches to information and intelligence sharing. Most of these participants were anti-fraud, IP crime or criminal intelligence sharing practitioners, although a couple represented relevant stakeholders at regulatory and government policy levels.

The study found that the foundation of effective intelligence sharing relationships is a combination of trust, competence in intelligence handling and mutual understanding between organisations. In order to overcome an array of challenges to collaboration, including a complex and commonly misunderstood legal framework, cultural resistance to sharing information and the lack of a comprehensive national strategy and standards for anti-crime intelligence handling and sharing, organisations employ a range of strategies. These include aligning their working practices to the National Intelligence Model as a default standard, formalising relationships through intelligence sharing agreements and committing resources to training both their own employees and staff in partner organisations to ensure that practitioners on both sides have the requisite skills and knowledge to share information in a competent and legal manner. There are significant risks remaining, however, in the interpretation and implementation of a default standard that was designed for law enforcement and in the context of forthcoming legislative change in data protection law.

Chapter One

Introduction

Background

Fraud and Intellectual Property Crime

Fraud affects all aspects of society, causing significant harm to its direct victims, to the wider economy and to society as a whole. The true cost of fraud is difficult to determine with accuracy for many reasons, not least of which are that it is, by its very nature, a hidden crime. Much fraud will remain undiscovered, and a significant amount of fraud that is discovered is not formally reported (NERA, 2000, pp.2-3), while methodologies for accurate measurement of it are still being formulated and refined (National Audit Office [NAO], 2016, p.20). Furthermore, a substantial amount of fraud is identified only by accident (Association of Certified Fraud Examiners [ACFE], 2016, p.21). In some areas, it has been difficult to distinguish between the crime of fraud and non-criminal activity: statistics and reports of tax and benefit fraud are still routinely conflated with those for errors (NAO, 2015, p.11), while many organisations and individuals also attribute losses to error or misfortune rather than crime (Levi, 1987, p.27). There are numerous different routes and sources for collecting and recording fraud data, all using different approaches and definitions, and many gaps where little or no data is collected at all. The differences in methodology can impact on the quality and reliability of some of this data (Levi, Burrows, Fleming & Hopkins, 2007, p.15). Even within government departments' central reporting of data, fraud is underestimated and inconsistently reported, with the NAO (2016, p.5) observing that some departments reported no fraud losses to the Cabinet Office for the data that it had started to collect, despite reporting it elsewhere for the same period.

Despite these problems, there are resources and research that we can use to get an overall understanding of the scale of the issue, at both national and international levels. In the UK, the national crime statistics in England and Wales show that 621,000 fraud offences were recorded by law enforcement agencies (Office for National Statistics [ONS], 2016, p.22) and provides an official estimate that 5.8 million offences of fraud and computer misuse occurred in the year to March 2016 (pp.38-39). The most recent attempt at a comprehensive national estimate of the cost of

fraud assessed the annual cost to the UK economy of £193 billion, with the private sector losing £144 billion, the public sector £37.5 billion and the remainder split between individuals and the charity sector (UK Fraud Costs Measurement Committee, 2016, p.11). That study revived the approach taken by the former National Fraud Authority [NFA] for which the most recent official estimates of the annual cost of fraud had been £52 billion (2013, p.2) and £73 billion (2012, p.7) respectively. Even these estimations do not cover all types of fraud, or all industries.

At the international level the challenges to measurement are greater still, although there are still estimations to which we can refer. One regular assessment is the biennial study conducted by the ACFE which surveys the cost of occupational fraud. The 2016 report estimated that the average organisation loses 5% of its turnover to fraud and posits that, extrapolated to global Gross Domestic Product [GDP], the annual cost to the world economy equates to $3.7 trillion (ACFE, 2016, p.8). Although there are methodological issues with the survey, the 5% figure remains consistent both with previous editions (ACFE, 2014; ACFE, 2012; ACFE, 2010) and with estimates by other researchers using alternative approaches (Button & Gee, 2013, pp.16-17).

Cybercrime, which can involve both fraud and intellectual property crime, is also a significant problem, with a recent international survey of over 6,000 organisations reporting that 32% had been victimised in the last year (PwC, 2016, p.9). Other research suggests the global average cost of a cyber-attack on an organisation to be as high as $6 million (Juniper Research, 2015, p.2), and that the global cost of data breaches will exceed $2 trillion by 2019. It has been reported that 34% of cybercrime targeting UK companies is related to intellectual property crime (Centre for Economics and Business Research, 2015, p.7). Intellectual property crime itself is difficult to put a cost to, as it covers a diverse array of criminality from corporate espionage and information theft to the trade in counterfeit goods including, most prominently in the UK, tobacco, alcohol, clothing, shoes and DVDs [Digital Versatile Discs] (IP Crime Group, 2015, p.6). Nationally and internationally the trade involves a more extensive range of goods including food, consumer electronics and pharmaceuticals, and there are documented links between intellectual property crime and organised crime syndicates (IP Crime Group, 2014, pp.24-25). Consumer entertainment-focused intellectual property crime increasingly involves the delivery and consumption of copyrighted entertainment material, including music, film and television content, through online streaming and away from the distribution of physical

media (Federation Against Copyright Theft [FACT], 2012b, p.5). Although there are no readily available comprehensive data on the losses to the UK economy, the costs have been estimated at £1.3 billion per year in respect of counterfeit goods alone (National Crime Agency [NCA], 2015, p.26).

More comprehensive estimates are available beyond the UK, perhaps most notably that intellectual property crime costs the US economy approximately $300 billion per year (IP Commission, 2013, p.2). The Organisation for Economic Cooperation and Development [OECD] (2008, p.114) estimated the value of the global trade in counterfeit and pirated goods to be $200 billion in 2005. A study commissioned by the International Chambers of Commerce built on the OECD methodology and extended it to domestic and internet-based counterfeiting and piracy. This produced an estimate of the cost of these crimes falling between $455 billion and $650 billion in 2008, with wider economic damage for the G20 economies in excess of $125 billion per year and 2.5 million jobs lost (Frontier Economics, 2011, pp.46-48). Furthermore, it projected that the cost of counterfeiting and piracy could increase to as much as $1.7 trillion by 2015.

These figures, which generally exclude wider associated costs, demonstrate the devastating damage that these crimes cause to the national and global economies. As such, they exemplify the need for effective action across all sectors to combat these crimes, of which information sharing is an essential component.

The Fraud Review and the Subsequent Environment for Combating Fraud

The sharing of information and intelligence has long been recognised as being of pivotal importance in combating fraud and similar crimes. Indeed, they are strategies of great value in combating many types of crime. However, where fraud and intellectual property crime are so widespread, affecting all aspects of society and impacting on organisations across all sectors and industries, it takes on particular significance. The UK's Fraud Review (Fraud Review Team, 2006b) placed significant emphasis on the need to improve cross-sector information sharing and devoted substantial coverage to issues of information, intelligence and data sharing. Since the Fraud Review was published the need for, and commitment to, improved collaboration and exchange of information and intelligence between organisations and agencies has been repeatedly restated as a central tenet in numerous official strategies for combating fraud and intellectual property crime (National Fraud Strategic Authority, 2009, pp.34-39; NFA, 2011b, pp.19-20; Cabinet Office, 2011a,

pp.12-13; Cabinet Office, 2011b, pp. 37-38; Fighting Fraud Locally Oversight Board, 2011; p.14; Home Office, 2011, p.21; Home Office, 2013, p.10; CIPFA, 2016, p.8).

The Fraud Review (2006, pp.76-77) observed that, while information about fraud is gathered by organisations other than law enforcement agencies, there are inadequate mechanisms or strategies in place to allow effective intelligence sharing between police forces, let alone between private sector organisations and the police. Despite this long-standing recognition that information sharing is an essential strategy for preventing and investigating economic crime, and the repeated inclusion of it within anti-crime strategies in the years since the Fraud Review, it is not clear that the situation has significantly improved.

The Fraud Review was the most comprehensive review of the fraud problem, and the infrastructure and environment for combating it, in recent years. It made a total of sixty-two recommendations with respect to improving the national response to fraud, including in the following key areas:

- creation of a National Fraud Strategic Authority [NFSA] to provide a strategic lead on the response to fraud and to measure the extent of the problem
- creation of a national fraud reporting centre to receive reports of fraud and to create and disseminate warnings, statistics and intelligence packages
- for the government and the NFSA, in consultation with the Information Commissioner's Office [ICO], to produce guidance on data sharing for public authorities
- for public authorities to give primacy to the common law position on data sharing
- establishing a National Lead [police] Force for fraud to act as a centre of excellence
- additional recommendations, and a recurring emphasis, on measures to enable and encourage greater information sharing (Fraud Review Team, 2006b).

Following publication of the Fraud Review, a number of actions were taken by the government which did significantly impact the response to fraud. Not least of these was the passing of the Fraud Act 2006, which significantly simplified the law with respect to fraud, introducing clearer offences. The Act was not a consequence of the Fraud Review, but rather the result of a Bill that was concurrent to it which arose from

a prior recommendation from the Law Commission (Farrell, Yeo & Ladenburg, 2007, p.2; Law Commission, 2002, pp.2-4). Additional legislative changes introduced after the Fraud Review included the introduction of the Bribery Act 2010 and, significantly, provision within the Serious Crime Act 2007 [SCA] for public authorities to share information with private sector organisations designated as Specified Anti-Fraud Organisations [SAFOs] (Home Office, 2015, p.7). The government also implemented several key Fraud Review recommendations, including establishing the NFSA (which later became the NFA), nominating the City of London Police [COLP] as the National Lead Force for fraud and establishing the National Fraud Reporting Centre (later renamed Action Fraud) and the National Fraud Intelligence Bureau [NFIB] within the COLP (HM Treasury & NAO, 2008, p.7). In addition, the Serious Organised Crime Agency [SOCA] was replaced by the NCA in 2013, with the new agency having an Economic Crime Command and a National Cyber Crime Unit within its operational structure (NCA, 2016, p.7).

However, not all developments were positive or permanent, with actions in a number of areas never fully implemented or subsequently rescinded. Most notable was the government's decision to abolish the NFA in 2014, resulting in the cessation of the publication of annual official measurements and estimates of the cost of fraud to the economy (Fraud Advisory Panel [FAP], 2016, p.6). Furthermore, following abolition of the NFA, there appears to be no overall coordination or strategic direction underlying ongoing collaborative initiatives between the government and private sector (FAP, 2016, p.8). There has also been limited engagement between public authorities and the private sector through the legal gateway established under the SCA. Only six bodies were designated as SAFOs when the gateway was established and the NFA reported in 2010 that there was limited use of this, with some major authorities – notably HM Revenue & Customs [HMRC] and the Department for Work and Pensions [DWP] – hesitating to share information with SAFOs despite the clear gateway being in place (NFA, 2010a, pp.14-17). A subsequent review of the use of the gateway indicated that neither HMRC nor the DWP were sharing information with SAFOs five years later, a full eight years after establishment of the channel (ICO, 2015a, p.15). The review also reported a disparity between the level of sharing reported by public authorities and that which the SAFOs themselves reported as taking place, concluding that this discrepancy was due to lack of understanding of the legal channel by public bodies (ICO, 2015a, p.5).

Legal Channels for Information Sharing

The legislative infrastructure surrounding the sharing of personal data in the UK is complex, convoluted, opaque and not widely understood. This greatly complicates the prospects for, and process of, greater collaboration for combating economic crime.

Public sector organisations are restricted to sharing within the extent of their legal powers (Law Commission, 2014, p.7). These powers are generally derived from statute, although in many cases these do not expressly cover data sharing (ICO, 2011, p.11). Public bodies' legal powers to share information may derive from:

- an express obligation to share
- an express power to share through a legal gateway defined by statute
- implied powers to share (ICO, 2011, pp.11-12)
- non-statutory powers (such as common law) (Law Commission, 2013, p.48).

Legal gateways are statutorily provided channels to enable public bodies to share data within specific circumstances or conditions (Fraud Review Team 2006a, p.125; Kennedy, 2007, p.383). These add significant complexity to the issue of data sharing as there are manifold gateways in place. The Law Commission found there to be in excess of sixty gateways for the DWP spread across more than twenty pieces of legislation (2014, p.26) and over two hundred and sixty for HMRC (2014, p.130). Furthermore, these are discretionary and there is no obligation for public bodies to share even if a gateway, specific or general, is in place (Department for Constitutional Affairs, 2011, p.21). The picture is complicated further as it is not always clear which law takes precedence in many circumstances, which can be problematic if determining which legal gateways exist, or whether these override obligations to keep data confidential. A more general gateway exists for public sector bodies under s.17 and s.115 of the Crime and Disorder Act 1998, allowing agencies to share information to enable them to prevent crime within their respective areas of responsibility (Brooks, Moss and Pease, 2003, p.8; Wenjing, 2011, p.365). Another broad gateway that was developed to allow public bodies to share information with the private sector for the prevention of fraud was under s.68 of the SCA, which allows sharing with private sector entities designated as SAFOs. However, as noted above, only six organisations were recognised as SAFOs when the legislation was introduced. Although the list has since been extended, only eleven SAFOs are currently

recognised (Home Office, 2015, p.20) and the gateway is still under-used by public authorities with respect to these as outlined above. Finally, there are common law powers that enable public bodies to share data. However, there is both considerable uncertainty as to their extent and application, and the Law Commission's (2014, p.86) consultation on information sharing found that the plethora of statutory gateways had resulted in the perception that there was no power to share information where no specific gateway was in place.

From a legal perspective, the situation is more straightforward for private sector organisations in that they have a general ability to share information so long as this is done within the constraints of the law (ICO, 2011, p.12). For both public and private sectors, the main legal parameters within which any otherwise legally permitted sharing may take place are the constraints of the Data Protection Act 1998 [DPA] and the law on confidence as derived from Article 8 of the European Convention on Human Rights, although some entities may be subject to additional constraints such as that of legal privilege (Law Commission, 2013, p.25).

While the DPA is a constraint on sharing, it does contain an important exemption from the rules on how personal data may be processed and disclosed under s.29 of the Act, which include exemptions for the prevention and detection of crime and for the apprehension or prosecution of offenders (ICO, 2001, pp.42-43). This provides a valuable channel to facilitate qualifying disclosures, although it is not a gateway that allows sharing in its own right (Law Commission, 2014, p.14).

There is considerable complexity within the law on data sharing, especially where this involves public authorities. This can impact on their ability and willingness to collaborate with other organisations, in both public and private sectors, for the prevention or investigation of economic crime. The law continues to develop in this area, with another legal gateway having recently been introduced through parliamentary legislation. Part Five of the Digital Economy Act 2017 contains a provision for an information sharing gateway between public bodies for the prevention, detection and investigation of fraud against a public authority, or the pursuit of sanctions. The sharing of information using this gateway, will be restricted to 'specified persons' to be defined under subsequent regulations, and a further code of practice will be issued setting out rules for use of the gateway (HM Government, 2016, pp.31-32). Such a structure for the proposed gateway does not suggest that

the government is moving in the direction of enabling more general gateways to assist in the fight against economic crime, or towards simplification of statutory provisions.

It should also be noted that not all information sharing need necessarily rely on legislative gateways. An often overlooked issue within the debate is that a considerable amount can be achieved through the sharing of non-classified data (Hardouin, 2009, p.209), although this thesis is primarily concerned with how to share data that might have some restrictions upon its exchange.

Intelligence Sharing Failure

It is important also to acknowledge that information and intelligence sharing do not just present opportunities for improving the fight against crime, but that there have been, and will continue to be, serious consequences for organisations' failure to do so. We have unfortunately been witness to numerous examples of intelligence sharing failure that have had serious, and sometimes tragic, ramifications in recent years, in both the crime and security arenas.

Failures in intelligence sharing have been highlighted in recent terrorist attacks, such as those in Paris in 2015 (Corera, 2016, para.12; Camilli, 2015, paras.3-9) and, more recently, in Brussels in 2016 (Karagiannis, 2017). Intelligence sharing failures have also been highlighted in many serious criminal matters in the UK in recent decades; the recent inquiries into the Jimmy Saville scandal found that intelligence reports had not been made available to several police forces; doing so could potentially have prevented serious abuses or led to earlier identification of his crimes (Oswald, 2013, p.7). Some of the most significant recent fraud cases could also have been averted with better sharing of intelligence. The fraud resulting in the collapse of Enron, which had previously been one of the ten largest US companies with assets valued at $62 billion in September 2001 (Oppel Jr. & Sorkin, 2001, paras.1-2), in November 2001 could have been identified sooner with better information sharing and scrutiny; the information in Enron's tax filings indicated that it paid no tax as a non-profitable company, in contrast to the information published in its financial statements (Gladwell, 2007, paras.57-58).

The Madoff Ponzi scheme, the largest fraud in history with losses of $65 billion (Bandler & Varchaver, 2009, para.3), could also have been identified much earlier with adequate intelligence handling and sharing. The U.S. Securities and Exchange Commission [SEC] missed several opportunities to investigate following direct

allegations and referrals made to it by a whistle-blower in 2000 and 2001, with the Boston office failing to send details to its New York counterpart (Markopolos, 2010, p.65) and through ignoring articles in the financial press questioning the integrity of the hedge fund (SEC, 2009, pp.74-77). These, and other, failings have had considerable ramifications, and serve as stark reminders as to the critical importance of intelligence and information sharing in combating fraud and other forms of crime.

Aims of the Research

This research concerns information and intelligence sharing for the purposes of fighting fraud and intellectual property crime, and how this may be encouraged, enabled and facilitated with a view to widening participation in anti-fraud information exchange. The importance and value of information and intelligence sharing for combating fraud is widely recognised. With the exception of a few sectors in the UK, however, it remains an under-employed and poorly understood strategy and whilst this remains the case the only winners are those who perpetrate these crimes.

This study will examine how information and intelligence sharing can be achieved successfully, with a view to promoting wider collaboration within the UK and beyond. Despite the recognition of the need for effective and widespread information and intelligence sharing between organisations and sectors to better combat issues of economic crime, and the significant economic and social incentives to do so given the scale of the problem, there remain considerable challenges that prevent many organisations from collaborating successfully. This notwithstanding, there are some organisations and anti-fraud information sharing schemes that do collaborate effectively. This research will examine the contemporary nature of these problems and consider how they may be overcome by examining models and strategies employed by those organisations that do have productive information sharing relationships in order that these may be adopted and modified by others to enable more widespread collaboration.

The research has been framed within the context of inter-organisational and cross-sector information sharing. The primary focus and purpose has been to understand the strategies and mechanisms that enable organisations to share information more effectively. Furthermore, the emphasis has been placed on seeking to understand how organisations that are not formally charged with law enforcement responsibilities may effectively collaborate with others on anti-crime issues. While information sharing is of significant importance within the law enforcement context, the aim has

been to examine strategies that may be employed by organisations that do not enjoy specific legal powers to enable them to share information for anti-crime purposes. Because of the lack of legislative provision for these entities, there remains considerable uncertainty about how they can collaborate effectively and legally. However, while this perspective has been taken, the law enforcement arena has not been disregarded within the research. Non-law enforcement organisations can learn a lot from the intelligence handling and sharing arrangements of the police and similar agencies, and vice versa. Of equal importance, for many organisations across all industries and sectors, anti-crime information sharing may necessarily involve collaboration with law enforcement agencies. Finally, the focus has been on information sharing within the UK, although cross-jurisdictional issues have inevitably arisen. This has primarily been for pragmatic reasons. Information sharing is a complex subject, with many challenges within the UK alone, and many of the issues become significantly more complicated when multiple jurisdictions are taken into account. It would not have been feasible to seek to address these issues on both national and international scales within a project of this size. Many of the issues and findings will, however, have relevance beyond the UK.

The research sought to address the following questions:

1. What is the contemporary nature of the barriers, both real and perceived, that impede effective anti-economic crime information and intelligence sharing between organisations, industries and sectors in the UK?

2. What potential strategies and solutions may be effective in helping to overcome these barriers, and what approaches have been effective to promote anti-crime collaboration?

    a. What types of strategy and solution could be employed to overcome the barriers to effective information and intelligence sharing?

    b. What can be learned from the models of successful existing information sharing partnerships, and can their approaches be translated into wider use in other industries and sectors?

3. How can professional practice be improved at the strategic and policy levels to help overcome the present impediments to wider information and intelligence exchange?

A significant amount of work has been conducted, and remains ongoing, into promoting greater information sharing between public authorities in the UK. Therefore, the emphasis for the research will be on promoting collaboration involving private sector organisations (and not-for-profit organisations by extension). However, the research has aimed to take relevant learning from public sector schemes into account where relevant, and does specifically include collaboration between public and private sector entities.

Key Definitions

In order to examine the sharing of data, information and intelligence, it is useful first to consider what they are. The Concise Oxford English Dictionary defines data as 'facts and statistics used for reference or analysis' (Soanes & Stevenson, 2006, p.364), a simple definition that infers the raw nature of data. Jennex (2009, p.6) defines it as 'basic, discrete, objective facts such as who, what, when, where, about something'. Rowley (2007, pp.171-172) observes that data in itself is void of meaning, that it is not processed or organised, whereas information is structured and has been processed in order to give it contextual meaning, relevance and value; it is the relational connection between data from this processing that endows this meaning (Bellinger, Castro & Mills, 2004, p.2).

Intelligence is perhaps a more complex concept to define. Historically, intelligence has been closely associated with the military setting, with references to, and guidance on, intelligence collection stretching back to antiquity. The final chapter of Sun Tzu's (n.d./1971, pp.144-149) famous treatise *The Art of War* concerned espionage, and the use of intelligence in military matters is documented back to 19th century BC in Chinese military history (Sawyer, 1998, p.7).

Despite such a long history, the definition of what constitutes intelligence is not settled, whether in the military, criminal or other contexts. Some definitions err toward the outcome, in that intelligence informs action, whereas others lean towards processing and intelligence products, averring intelligence to be information that has been processed and analysed (Warner, 2002, p.16). Wheaton and Beerbower (2006, p.329) argue in favour of a definition that focuses on the purpose of intelligence being

to reduce uncertainty, while Brown (2007, p.340) suggests that intelligence is information imbued with the quality of *significance*. Johnson (2006, p.120) holds that intelligence must be capable of being turned into *useable* information. For Warner (2002, p.20), another key element of intelligence is *secrecy*. This has some merit, although it does ignore that much information that comprises intelligence is gathered from publicly available sources; the concept of *open-source intelligence* is widely used and accepted in the criminal intelligence field, amongst others. However, these concepts of significance, secrecy and its utility to inform decision making or action are central to most definitions of intelligence. Corporate intelligence is geared towards two prime purposes: helping organisations manage risk, which would include crime risk, and to assist in exploiting opportunities (Strachan-Morris, 2013, p.120). Most definitions of intelligence, by nature, work on the inference that the intelligence is correct, whereas it has long been recognised that much intelligence can be false, contradictory or subject to uncertainty (Clausewitz, 1832/1989, p.117); a consideration relevant to both military and criminal intelligence and a reason for applying both caution and controls.

The fight against economic crime can involve, and benefit from, the prudent and legal exchange of data, information or intelligence. There can be different approaches, processes and channels that apply to the exchange of these, although in many situations the exact distinction between data and information, or information and intelligence, may not be clear or consistent, and this is regularly featured in discourse on the subject. At certain levels, the distinctions are of practical importance, such as in considerations of bulk sharing and anonymisation which may be feasible for data sharing, but usually less suitable for intelligence. At a more theoretical level, the distinction may be less significant, in that the delineation between the concepts of intelligence and information may be indistinct or even interchangeable. This thesis follows this trend in that the terms may sometimes be interchanged when sharing is being discussed at a more general or theoretical level and the distinction is less important, but with more discriminate application when the technical or practical differences make it appropriate to do so. This notwithstanding, for the purpose of this thesis, the term *data* refers to raw facts, *information* to data which have been processed and given contextual meaning and value, and *intelligence* as data or information that have been analysed and processed and are considered relevant and useable to inform decision making or action in the management and response to economic crime incidences or risks.

As this thesis is concerned with both fraud and intellectual property crime [IP crime], the term *economic crime* has been used to refer to both collectively.

Structure of the Thesis

The remainder of this thesis has been structured into chapters as follows.

Chapter Two presents a literature review examining issues of information and intelligence sharing from a number of perspectives including knowledge management, e-government collaboration and information sharing projects within the criminal justice and other fields. It considers barriers to, and enablers of, information sharing identified in past studies before taking a concise look at aspects of intelligence handling theory and practice.

Chapter Three sets out the methodology followed in this study, which was conducted in two phases. The first was a case study of FACT and the second a series of semi-structured interviews with representatives of other organisations as active participants in the practice or process of information and intelligence sharing for anti-crime purposes.

Chapter Four is the first of four chapters setting out the findings of the research. This chapter discusses the key findings relating to challenges and barriers to information sharing with respect to economic crime. It also sets out findings relating to the legislative framework for information sharing and the problems within this.

Chapter Five outlines FACT as an organisation and provides an overview of its mission and structure. It examines some of the key functions and processes of the organisation and how these pertain to its approach to successful information sharing relationships with other agencies and sectors.

Chapter Six details key findings from both phases of data collection in respect to the strategies and methods used by organisations to build and maintain effective information and intelligence sharing relationships with others and to overcome the challenges and barriers to collaboration.

Chapter Seven discusses findings from the data relating to issues of competence in intelligence handling, education and training. These issues are all central to effective

intelligence sharing relationships. The chapter also looks at the early indications of the embryonic professionalisation process emerging in the field.

Chapter Eight presents a high level discussion of the findings, examining the key issues arising in five overarching themes: the barriers to information and intelligence sharing; the legislative framework; standards; relationship management; and the subject of professionalisation. It also illustrates the structures of several models of information sharing that arose from the data; models that can facilitate inter-organisational intelligence sharing between two, or between many, different parties.

Chapter Nine presents the overall conclusions of the study, assessing at a high level how the findings respond to the original research questions. It also identifies how the research has made a contribution to knowledge in the area of anti-economic crime information and intelligence sharing.

Chapter Two

The Practice of Information Sharing and Intelligence Handling

Introduction

Information and intelligence sharing has long been identified, within both the literature and within public policy and debate, as an essential component in the fight against fraud. There are parallels with similar debates and initiatives to promote information sharing within the context of many other types of crime, from murder investigations to counter terrorism, and with other forms of governmental collaboration concerned with non-law enforcement issues.

Numerous factors have contributed to information sharing being highlighted as a necessity within law enforcement, leading to a greater political impetus to promote and implement information and intelligence sharing initiatives. From the role that data sharing can play in risk assessment and the focus on harm prevention within social policy (Bellamy, 6 & Raab, 2005, p.396) to widespread criticism levelled at the government and law enforcement bodies for failing to share relevant information that could have prevented tragedies, such as in the case of the Soham murders (Bichard, 2004), these arguments have become prominent and regular. Many other high profile cases, including murder, fraud, child abuse and more, have pushed information sharing higher up the political agenda (6, Bellamy, Raab, Warren & Heeney, 2006, p.406; Bellamy, Raab & 6, 2005, p.57). The need for, and activity towards, the sharing of intelligence between agencies at national and international levels were highlighted in the wake of the September 11th attacks on the World Trade Centre in New York (Gottschalk, 2005, p.617; Kim & Lee, 2006, p.370), which raised the political stakes even further. It has been argued that the political drive to increase information sharing and collaboration stems from widely-held perceptions that such high profile failings have resulted from excessive emphasis being placed upon privacy and confidentiality (6 et al, 2006, p.406). This has a ring of truth to it, and may help to explain why collaboration has not occurred even where channels have existed to allow for information sharing; Grabiner (2000, pp.20-21) commented on the disjointed exchange of information between public sector agencies despite the existence of legal gateways to enable it.

A literature review was conducted in order to examine the understanding of information sharing issues within both the anti-fraud and wider contexts. There has been relatively little published within the academic literature concerning anti-fraud information sharing issues, although there is a small, but growing, body of knowledge in the grey literature. However, information sharing has been discussed, debated and trialled in many fields and sectors, and there are relevant lessons that can be drawn from these and applied to the promotion of anti-fraud collaboration.

This chapter sets out the findings of the literature review with four main focal points. The first examines literature concerning information sharing within the contexts of organisational knowledge management and transfer, and the burgeoning field of e-government collaboration. It then proceeds to examine some key learning points from a number of information sharing projects from around the world, in both law enforcement and non-law enforcement environments, identifying the challenges that they faced and factors that contributed to their success. This is followed by a review of the current state of anti-fraud information sharing in the UK, reviewing the primary challenges faced in sharing information between organisations and sectors for the prevention, detection and investigation of fraud. Finally, a brief review is conducted of two models within the theory and practice of intelligence handling: the intelligence cycle and the National Intelligence Model [NIM].

Knowledge Management, Sharing and Transfer

The first area examined was knowledge management, sharing and transfer. Knowledge management is the processes of creating, using, storing, distributing, sharing and understanding knowledge (Bock, Zmud, Kim & Lee, 2005, p.88; Gottschalk, 2006, p.381). In planning for the effective management of organisational knowledge, Cabrera and Cabrera (2002, p.691) suggest that managers should explicitly consider the motivations and barriers to information sharing, and how these can be overcome, before investing in knowledge management systems. By implication, information sharing should be a prime consideration in organisations' management of information.

The concept of organisational ownership of information is central to both knowledge management and information sharing. Information has variously been described as being owned by organisations in terms of information products created by employees that should be used for the good of the organisation (Constant, Kiesler & Sproull, 1994, p.418), as a key strategic asset that is difficult for others to reproduce (Cabrera

& Cabrera, 2002, p.688) and as a source of organisational power (Cress, Kimmerle & Hesse, 2006, p.372). In the law enforcement context – which can be extended to a wider economic crime context – Gottschalk (2006, p.381) argues that knowledge is the most important resource in investigations, and that successful outcomes are highly dependent upon the availability of information. Jarvenpaa and Staples (2000, p.134) suggest that the concept of organisational ownership of information is not a social norm, but rather an organisational norm. Kolekofski Jr. and Heminger (2003, p.523) suggest that organisational norms will influence information sharing to the extent that sharing may occur regardless of potential barriers, such as lack of reciprocity, if the sharing organisation believes the process to be of benefit to it. A study by Bock et al (2005, pp.100-101) demonstrates that the greater the subjective norm to share information, employees will be more willing to do so, although it also found that employee attitudes would be positively affected by perceived reciprocity in the relationship. This could potentially be significant in respect of anti-fraud information sharing, suggesting that some of the cultural barriers that exist may be within organisations' power to overcome; it is more feasible for organisations to change their own norms than societal values.

It is important to recognise, of course, that there are different types of knowledge. A commonly used distinction is that of *tacit knowledge*, described as those types of knowledge that are harder to communicate and transfer, including skills and practical knowledge (Cabrera & Cabrera, 2002, p.690), and *explicit knowledge*, such as facts and records, that is more readily transferrable (Pardo, Cresswell, Thompson & Zhang, 2006, p.295). The majority of information sharing needs that prove challenging in the economic crime context would likely be in the form of factual data and records. As this is explicit knowledge, this should be more readily transferrable than other types of information. However, Ipe (2003, p.344) cautions that just because explicit knowledge can be more readily transferred does not necessarily mean that it will be shared. Furthermore, as many organisations are targeting resources towards sharing of tacit knowledge internally (Syed-Ikhsan & Rowland, 2004, p.95) this focus does not advance the prospects of inter-organisational exchange of explicit knowledge that would be of most benefit in combating economic crime.

Organisational knowledge transfer has been defined as "the process through which organizational actors – teams, units or organizations – exchange, receive and are influenced by the experience and knowledge of others" (van Wijk, Jansen & Lyles, 2008, p.832). It is the emphasis on the change and impact caused on the recipient

(Argote & Ingram, 2000, p.151; Argote, Ingram, Levine & Moreland, 2000, p.3) that suggests that knowledge transfer is more concerned with the exchange of tacit rather than explicit knowledge, and thus differentiates it from the end goals of information sharing, but there are still relevant lessons that can be drawn from these processes, especially with respect to the transmission of skills to enable information sharing. Kim and Lee (2006, p.370) suggest that *knowledge sharing* "requires the dissemination of individual employees' work-related experiences and collaboration between and among individuals, subsystems, and organizations; collaboration with other agencies and stakeholders". This incorporates the important element of collaboration into the equation. In line with the issues surrounding anti-crime information exchange, it has long been recognised that knowledge sharing is highly beneficial for organisations, which are more likely to succeed if they can transfer knowledge effectively (Argote et al, 2000, p.2), while van Wijk et al (2008, p.832) cite research indicating that knowledge transfer is more difficult between multiple organisations than internally.

Kim and Lee (2006, p.373) identify three cultural enablers that help facilitate knowledge sharing, these being trust, a clear organisational vision, and social networks. Van Wijk et al's (2008, p. 845) study demonstrated clear links between trust and the existence of strong relationships [between participants] and effective knowledge transfer, suggesting that this *relational capital* is the most significant factor enabling intra- and inter-organisational transfer. It has been recognised that participation in information sharing is strongly influenced by the levels of trust between parties (Canestraro, Pardo, Raup-Kounovsky & Taratus, 2009, pp.115-116). An important element of trust is the reliability of the source (Argote & Ingram, 2000, p.161). In a study of drivers and impediments to knowledge sharing in virtual communities of practice, Ardichvili, Page and Wentling (2003, pp.73-74) found that central to the creation of knowledge sharing networks was the establishment of institution-based trust establishing the principles and structures for sharing, and also the communication of the rules and standards by which participants should abide.

The establishment of a knowledge-sharing culture is also a noted requirement towards the success of sharing schemes. A study of public sector organisations in Malaysia reported a positive correlation between a knowledge sharing culture and the performance of knowledge transfer (Syed-Ikhsan & Rowland, 2004, p.107), while Gottschalk (2005, p.618) observes that, within the law enforcement context, there is a need for a culture that embraces collaboration. Fifteen years ago, Cabrera and Cabrera (2002, p.704) suggested that an environment that encouraged information

sharing was of greater significance to success than technology solutions that facilitate it. Unfortunately, it is also recognised that some organisations intentionally stifle opportunities for sharing information and knowledge for a range of reasons, from perceived threats to resourcing issues (Constant et al, 1994, p.401; Hatala & Lutta, 2009, p.12).

One further way of examining the issue is through the lens of information sharing as a social dilemma. Social dilemmas have two primary properties: there is a higher potential payoff for individual parties if they make selfish choices at odds with the greater good, but all parties are better off if every party cooperates rather than acting selfishly (Dawes, 1980, p.169). Government agencies share information for the generation of public goods (Lee & Rao, 2007, p.155), such as protection from crime. Private sector organisations share information in line with the underlying profit motive; minimising losses to economic crime can contribute to that goal. Social dilemmas apply to both of these contexts, and have been linked to the problems impeding these goals (Kalman, Monge, Fulk & Heino, 2002, p.127). Where information sharing is for the public good - such as reducing economic crime in both public and private sectors - there is the potential for every member of the group to benefit from the activity, regardless of their level of contribution. This is known as the *public-good dilemma* (Cabrera & Cabrera, 2002, p.693). In this situation, as not all members are required to collaborate in order to share the good, this increases the chance of members acting selfishly, rather than for the common good, which Cabrera and Cabrera (2002, p.693) refer to as the *deficient equilibrium*. A suggested means of overcoming this problem is to establish rewards and incentives for individual members in order to align the individual's interest with the greater good to ensure that collaboration becomes the optimum strategy for members (Cabrera & Cabrera, 2002, p.696; Cabrera, Collins & Salgado, 2006, pp.250-251).

Information Sharing in E-Government Collaboration

Information sharing is also a significant and highly relevant topic within the field of e-government collaboration, in which inter-departmental information sharing is essential. Cross-departmental anti-fraud information sharing in the UK remains a challenge, but there is a wider literature that discusses some of the challenges and enablers in government collaboration, some of which are relevant to the economic crime arena.

E-government collaboration and inter-agency working are increasingly common themes in modern government, with an extensive range of projects being undertaken to solve a range of complex and far-reaching issues, such as emergency response, online provision of public services, multi-partner environmental data exchange and cross-jurisdictional identity authentication (Chun, Luna-Reyes & Sandoval-Almazán, 2012, pp.7-9). In order to meet contemporary challenges, it is essential for government agencies and departments to collaborate (Degwekar, DePree, Beck, Thomas & Su, 2007, p.102; Zheng, Dawes & Pardo, 2009, p.43). Where these challenges involve multiple agencies, inter-organisational information sharing is required (Gil-Garcia et al, 2009, p.3) although there are many obstacles to such cooperation, ranging from legal restrictions to IT challenges. Despite numerous government initiatives over many years to promote interagency collaboration, the sharing of information between agencies has remained inconsistent (6 et al, 2006, p.407), indicating that there remains considerable work to do. Given recognition that achieving these aims will require a considerable overhaul of processes and the introduction of a comprehensive infrastructure to support information sharing (Landsbergen & Wolken, 2001, p.212; Pardo, Gil-Garcia & Burke, 2006, p.1), the limited progress is perhaps unsurprising.

The literature on e-government collaboration and government information integration examines the nature of the barriers that impede information sharing and collaborative projects, and provide useful classifications and perspectives that can be applied to economic crime collaboration. Dawes (1996, p.378) classified issues into three discrete categories: technical, organisational and political barriers. Some have added the additional distinction of legal barriers (Gil-Garcia, Chengalur-Smith & Duchessi, 2007, p.122; Gil-Garcia et al, 2009, p.3), differentiating elements that would have fallen under the political classification in the former analysis. Other analyses place emphasis on different elements again, such as the five-category analysis of Zhang and Dawes (2006, p.437) of technological, organisational, legal, policy and financial barriers. The explicit recognition of financial issues as a major challenge is important, and this is recognised by other commentators as being a significant impediment to governmental information sharing (Lam, 2005, p.519; Landsbergen & Wolken, 2001, p.209). Lam (2005, p.518) proposes a four-part classification of barriers to e-government integration, of strategic, technological, policy and organisational barriers. The inclusion of strategic barriers, including such factors as lack of ownership and governance, financial constraints and the lack of common objectives between collaborators (Lam, 205, pp.518-519) is an interesting proposition. However, while it

is clear that the wide range of barriers can be analysed in different ways (Figure 2.1), the actual barriers that are generally identified within these analyses do not differ greatly; they are merely attributed to different categories. Perhaps one overarching obstacle that is not commonly discussed elsewhere does emerge from the e-government literature, however: that inter-organisational information sharing and collaboration itself is an ambitious goal. It has been argued that this ambition, or perhaps over-ambition, is itself an obstacle to success (Lam, 2005, p.518; Zhang, Dawes & Sarkis, 2005, p.561). This may be a justified view, but the implications would be concerning with respect to improving multi-agency sharing to combat economic crime, although this can be managed to an extent through the setting of realistic interim objectives (Zhang et al, 2005, p.561).

Figure 2.1: Variant classifications of barriers to information sharing

While technology-related issues, such as incompatible legacy systems (Gil-Garcia & Pardo, 2005, p.192), are recognised as barriers to information sharing, it has also been argued that these types of barrier are of lesser magnitude than other challenges faced (Landsbergen & Wolken, 1998, p.5). This notwithstanding, other technical issues do provide lasting challenges to public sector information sharing, not least of which are data quality problems. These can include basic, but significant, complications like errors, incomplete and inconsistent data (Gil-Garcia & Pardo, 2005, p.190) and data accessibility issues, as well as more subtle and complex issues of contextual significance which can arise from different stakeholders' perspectives (Dawes et al, 2009, pp.394-395; Klischewski & Scholl, 2006, p.7). As such, it is argued that participants need to reach agreement on data quality matters within information sharing initiatives (Dawes et al, 2009, p.395; Klischewski & Scholl, 2006, p.2).

Some of the legal issues that surround anti-fraud information exchange were introduced in Chapter One. Many of these issues apply within the wider e-government collaboration context, not least of which is that of data protection legislation, of which the UK's is currently subordinate to the EU Directive on data protection (Otjacques, Hitzelberger & Feltz, 2007, p.34). However, such restrictions may not be the only relevant factor. Dawes et al (2009, p.398) argue that lack of legislative (and financial) support for public sector knowledge sharing initiatives is more challenging than legal restrictions, while Wenjing (2011, p.369) points out that some legal restrictions on public sector information sharing are necessary and desirable to mitigate risks inherent within it.

Cultural barriers are another prominent theme within the e-government collaboration literature, and it is clear that these are key issues that any information sharing initiative, in any sector, will need to tackle. Where governmental information sharing requires infrastructure to enable it, there are also concerns that there will inevitably be some resistance to any perceived centralisation that this entails (Lazer & Binz-Scharf, 2004, p.18). Furthermore, Pardo et al (2006, p.295) observe that the knowledge that would be shared through a collaborative arrangement is embedded within the culture of the sharing organisation, and that an effective information sharing initiative must find pathways through the different cultures and processes of the participating entities. Not only can different working cultures within public sector organisations impede sharing, but subcultures can too. Drake, Steckler and Koch (2004, pp.67-69) point out that different subcultures hold different norms and values and that these too can impede information sharing and undermine trust, furnishing an example of bureaucrats withholding information from politicians. This may help to explain why at least some anti-fraud information sharing drives in the public sector have failed, despite enjoying political support.

The literature also identifies some of the lessons learnt from public sector initiatives, and ways to overcome the challenges. Managers can overcome problems arising from participating organisations having different expectations and objectives by recognising at the outset that the parties will have different perspectives (Gil-Garcia et al, 2007, p.131); this links to the identified need for stakeholders to understand each other's needs and align goals. Creating an effective initiative requires the development and maintenance of relationships between participants (Pardo, Cresswell, Dawes & Burke, 2004, p.3; Pardo & Tayi, 2007, p.700), which can help maintain trust. This is essential in all cases, but especially where participants, and

therefore the network, may be distributed over a large geographic distance, which can itself be a barrier (Dawes et al, 2009, p.396), and where face-to-face contact in the early stages can help build lasting relationships. Building trust through such relationships is essential to make information sharing initiatives work, so much so that it has been proposed that at the planning stages of new collaborations, resources should be specifically allocated for building trust (Pardo et al, 2006, p.7). While this might prove a difficult concept to promote within the public sector, and perhaps within some private sector initiatives, it could prove to be resources well directed; Willem and Buelens (2007, p.597) found that a trusting environment would result in the sharing of more knowledge by participants, and also make the knowledge sharing more effective.

Information Sharing Schemes

Information sharing and collaboration schemes have been attempted, and studied, in a wide variety of contexts around the world. It is useful to examine the literature relating to some of these to examine the challenges - and solutions - encountered by such projects, as these may be pertinent to the economic crime arena. Some have encountered issues that were not anticipated at the outset. For example, Dawes, Cresswell and Pardo (2009, p.396) comment on a collaborative project involving government agencies and organisations providing facilities for the homeless in the US, whereby an agreement to share policies and practices was finally reached based on a common understanding on the protection of service users' identities. Unforeseen issues arose when a domestic violence shelter joined the scheme and pointed out that, from its perspective, the key issue was the protection of the facility's location rather than the identity of residents.

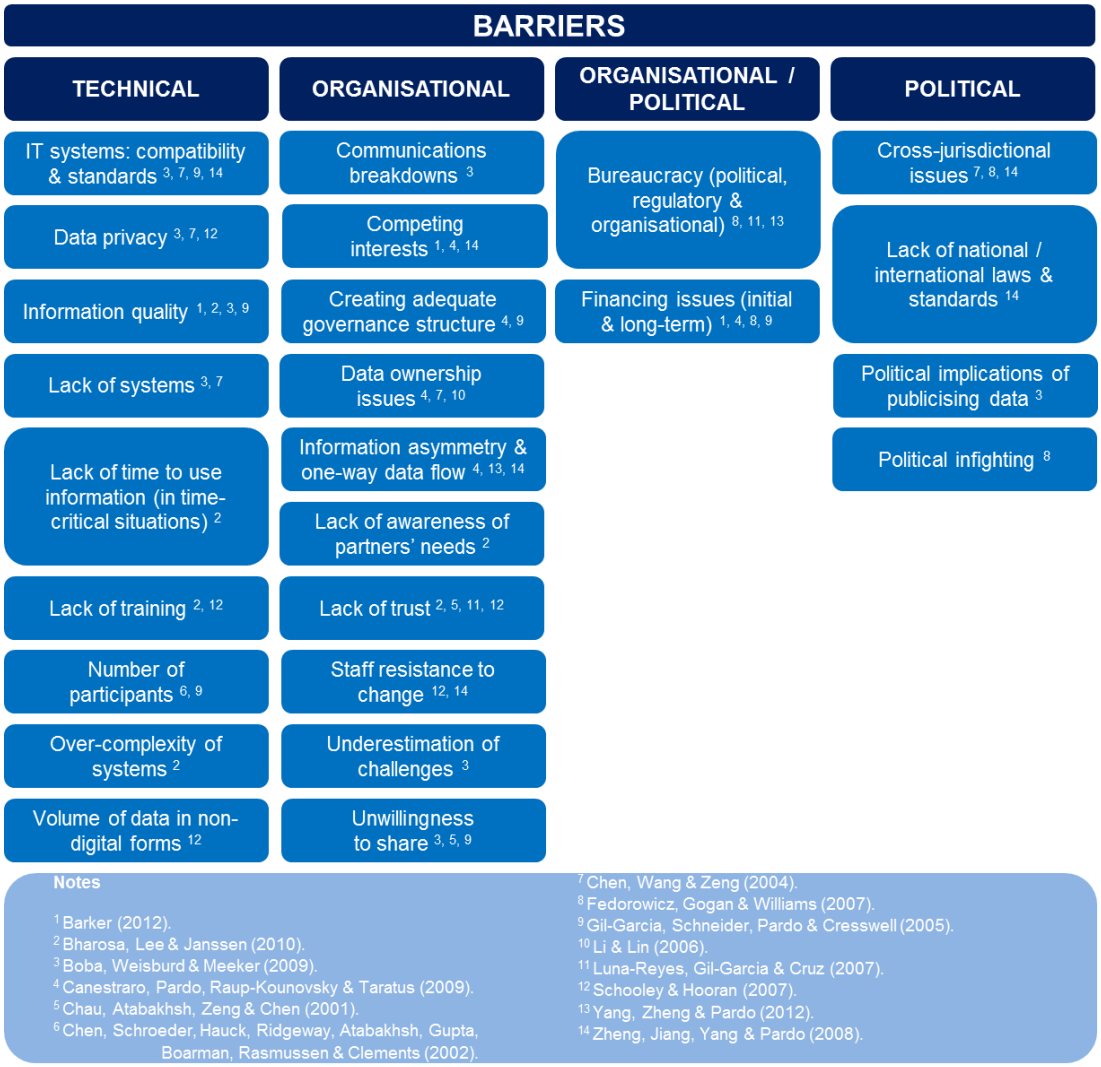
Significant multi-organisation information sharing projects have been conducted in such varied fields as emergency first responders (Fedorowicz, Gogan & Williams, 2007); disaster management (Bharosa, Lee & Janssen, 2010); communicable diseases (Chen, Wang & Zeng, 2004); telecommunications (Canestraro et al, 2009); e-government services (Luna-Reyes et al, 2007; Yang, Zheng & Pardo, 2012); food safety and product quality (Zheng, Jiang, Yang & Pardo, 2008); supply chain management (Li & Lin, 2006); and emergency medical services (Schooley & Horan, 2007). These projects were set within a range of different environments and circumstances, each of which presented different challenges. These included issues relating to the sharing of information between organisations across different sectors,

countries and jurisdictions, covering large territories and distances, and, in some cases, between large numbers of organisations.

There are also examples within the literature of information sharing schemes within the law-enforcement context, predominantly within the US. As with the arguments for information sharing to combat economic crime, there is recognition within the law enforcement arena that information sharing between agencies could improve their ability to fulfil their respective missions (Bajaj & Ram, 2003, pp.59-60; Bajaj & Ram, 2007, pp.29-30). However, there is also a potential tension between the traditional focus on the secrecy of intelligence and more recent emphasis on using intelligence more effectively – including information sharing – that came with the concept of intelligence-led policing (6, Bellamy, Raab, Warren & Heeney, 2006, p.423; Tilley, 2003, p.323). Experiences and lessons from these schemes can provide valuable insight into the challenges and facilitators of inter-organisational information sharing. Initiatives such as COPLINK (Chau, Atabakhsh, Zeng & Chen, 2001; Chen et al, 2002; Gottschalk, 2005, p.619; Zeng et al, 2003; Zhao et al, 2004, pp.625-631); California's COMPASS initiative (Boba et al, 2009); the Colorado Integrated Criminal Justice Information System (CICJIS) and the Delaware Justice Information System (DELJIS) (Gil-Garcia et al, 2005) and the Commonwealth of Pennsylvania Justice Network (JNET) (Cresswell, Pardo & Hassan, 2007; Gil-Garcia et al, 2005) demonstrate some of the issues faced by large scale information sharing schemes in the criminal justice arena.

The literature outlining these schemes highlights some common themes amongst many projects, alongside other points of consideration in light of their potential to impact information sharing within the anti-fraud arena. A wide range of barriers and challenges to successful sharing were faced by these collaborations, including those summarised in Figure 2.2.

Figure 2.2: Summary of barriers identified in information sharing schemes



Issues around computer systems and compatibility problems arising from partners using different systems, software and data formats arose in several cases. General system incompatibility issues, and problems relating to legacy systems, were identified as clear challenges to successful collaboration (Boba et al, 2009, p.35; Chen et al, 2004, p.336; Zheng et al, 2008, pp.93-94), in line with findings from the e-government collaboration literature. There were other barriers described with respect to the technology for information sharing too. These ranged from the lack of systems available – with inevitable implications for the effectiveness of information sharing – for alerting and reporting between organisations in respect of outbreaks of West Nile Virus and Botulism (Chen et al, 2004, p.336) to problems where the systems that were in place were over-complex and not user-friendly (Bharosa et al, 2010, pp.62-63).

Concerns over the quality of information shared, and shareable, by partners was also a prominent challenge for many projects. General concerns about poor quality data were an issue in the DELJIS project (Gil-Garcia et al, 2005, p.7), and these have been echoed more recently as a major challenge in the anti-fraud field by the UK's Insurance Fraud Bureau [IFB] (Barker, 2012, p.20). Such issues are compounded by, and contribute to, lack of trust in the quality of information supplied by partners during information sharing as well as to fear both of information overload and of being swamped by irrelevant data (Bharosa et al, 2010, pp.56-57). Parallel to the issue of system incompatibility, these problems are not helped where partners within a scheme store data in a wide variety of formats, some of which may be uncommonly used. In the COMPASS information sharing project in California, this very issue complicated and confounded initial attempts to identify the nature and formats of data collected and stored by participants in the scheme due to the sheer quantity of formats employed (Boba et al, 2009, p.29).

Another data-related problem experienced within the emergency medical services field was the sheer volume of information recorded and transmitted in non-digital form, including hand-written and spoken information (Schooley & Horan, 2007, p.771). Due to the nature of these communication media, they are not readily transmissible or shareable at a large scale, although may well contain important information that partner agencies might benefit from.

Data privacy issues were highlighted in several projects, with the handling of sensitive data and confidentiality prime concerns (Boba et al, 2009, p.29; Chen et al, 2004, p.336). Fear of potential legal or political action arising over data privacy matters was an issue for the collaboration in an emergency medical services project (Schooley & Horan, 2007, p.778).

A number of other technical obstacles were identified across the projects, not least of which, for some of the larger schemes, were complexities arising from involving large numbers of participants (Cresswell et al, 2007, pp.122-123; Gil-Garcia et al, 2005, p.7), many of whom would be using data in different ways to their partners (Chen et al, 2002, p.274). Other notable problems included lack of training for staff in how to use information sharing systems and, in time-critical situations such as those experienced in disaster management, the lack of time available for people to absorb information shared by partners (Bharosa et al, 2010, p.57).

The literature also reflected a variety of organisational and cultural barriers that the schemes came up against. Fundamentally, lack of trust amongst partners was an issue reported in several cases (Canestraro et al, 2009, p.116; Chau et al, 2001, p.3; Luna-Reyes et al, 2007, p.813; Schooley & Horan, 2007, p.775). Similarly, another challenge was that of competing interests for private sector participants which could interfere with their willingness to share information (Canestraro et al, 2009, p.116; Zheng et al, 2008, p.95). This factor had been experienced by the UK's IFB, where insurers perceived their own fraud management capabilities as a competitive advantage, disregarding the bigger picture (Barker, 2012, p.21). Some projects experienced a general unwillingness of some partners to participate and share information (Boba et al, 2009, pp.29-30; Chau et al, 2001, p.3; Gil-Garcia et al, 2005; p.7), and Li and Lin (2006, p.1643) reported perceptions held by some organisations that disclosing information to others represented a loss of power. Related issues were problems of information asymmetry between participants that were information rich and poor (Yang et al, 2012, p.S54), and concerns that in some cases the information flow was in one direction only (Zheng et al, 2008, p.95). In one case, staff unwillingness to share was identified as being attributable to internal communications failures within organisations, whereby senior officers supported the collaboration but failed to communicate the authorisation to share data to their subordinates (Boba et al, 2009, p.31). Lack of incentives for organisations to share was cited as a challenge to participation in one scheme (Zheng et al, 2008, p.95), while another reported that sharing suffered due to lack of feedback from recipients and failure to acknowledge the contribution that information received had made to successful outcomes (Bharosa et al, 2010, p.58).

The Californian COMPASS project found that the organisations involved underestimated the extent of the challenges at the commencement of the project (Boba et al, 2009, p.30). A disaster management project reported problems arising from collaborating agencies' lack of understanding of the other participants' needs, and were unsure what information would be useful to share and what would be unhelpful and distracting (Bharosa et al, 2010, pp.56-59). Issues of ownership of shared data were also reported (Chen et al, 2004, p.336), as was the problem of staff resistance to change resulting in information sharing tools and equipment being unused or underused (Schooley & Horan, 2007, p.774; Zheng et al, 2008, p.94).

A major issue identified in several projects related to the governance structure. Challenges ranged from lack of an overall decision making body in the JNET scheme

to problems of composition of the board; the DELJIS board included technical staff that were unable to make decisions on behalf of their own organisations (Gil-Garcia et al, 2005, p.7). Creation of an appropriate governance structure was identified in one instance as the single greatest challenge faced (Canestraro et al, 2009, p.122).

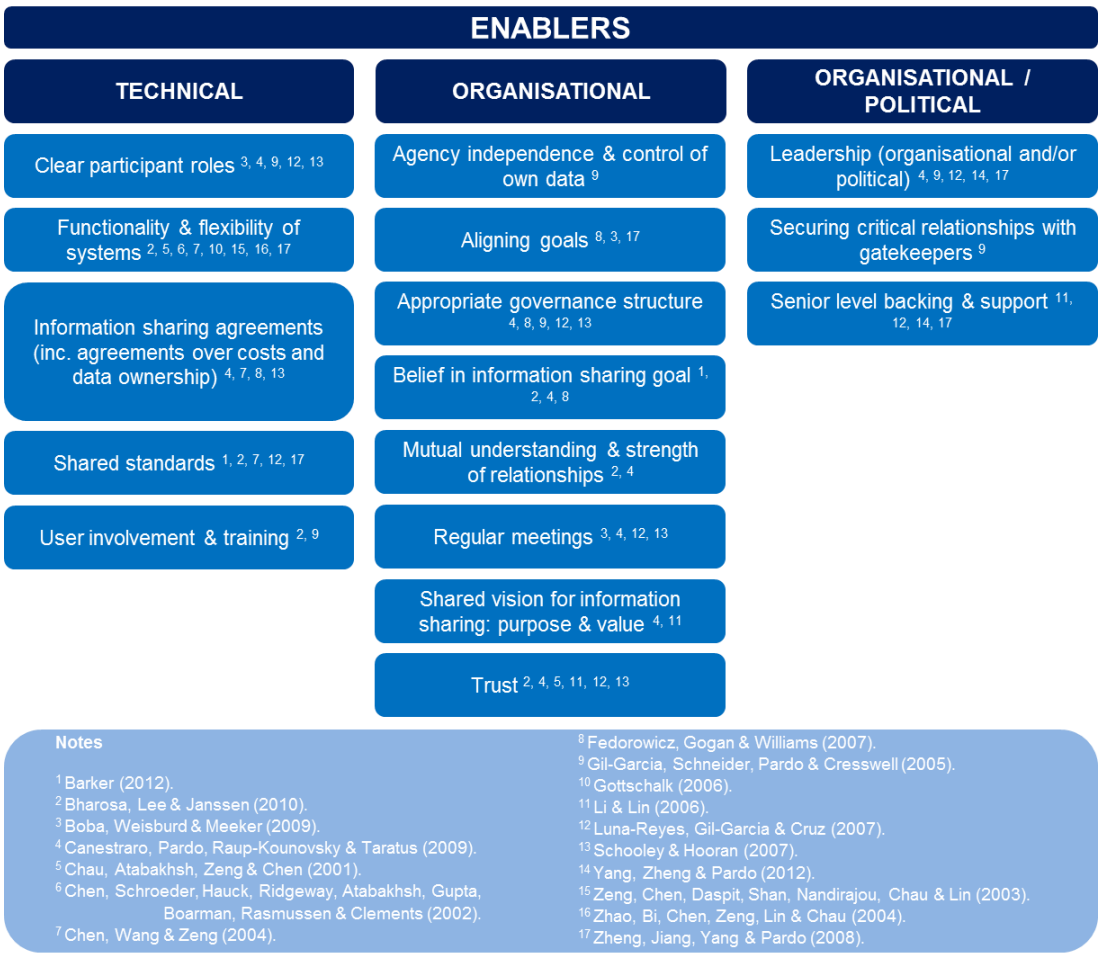
Straddling the divide between organisational and political barriers – depending upon the context within which the projects were situated – was the issue of excessive bureaucracy. This ranged from problems caused by the wider regulatory environment (Luna-Reyes et al, 2007, p.819) to internal organisational rules requiring formal assessment of each instance of sharing, even where the sharing was between different parts of the same department (Yang et al, 2012, p.S55).

Finance was also a major challenge (Fedorowicz et al, 2007, p.796; Gil-Garcia et al, 2005, p.7). Funding challenges were not restricted to initial financing, but extended to the costs of maintaining the project and its sustainability (Boba et al, 2009, p.31; Gil-Garcia et al, 2005, p7). Lack of funding for future development was an issue for the CICJIS project (Gil-Garcia et al, 2005, p.7) and problems of different agencies vying for control of funding arose elsewhere (Fedorowicz et al, 2007, p.797). Funding issues, even when they are indirect, can also have unexpected implications for schemes; the IFB cites as a major barrier to its success the cuts to police budgets for tackling fraud (Barker, 2012, p.20).

A small number of political problems were highlighted by some projects, but these issues can present potentially significant obstacles to success. These generally related to issues arising from operating across multiple jurisdictions. The US-based CapWIN project for emergency first responders suffered political obstacles relating to funding and other issues, involving numerous government bodies at state and local levels, delaying the scheme for many months, and political factors had to be incorporated into the project's design and governance (Fedorowicz et al, 2007, p.796). Cross-jurisdictional issues add another layer of complexity to many information sharing projects, be this across regional, national or international boundaries (Chen et al, 2004, p.336). The lack of international laws unifying standards across nations was cited as perhaps the most significant challenge facing efforts to encourage data sharing at a global level (Zheng et al, 2008, p.95). At a more localised level, political concerns over potential implications and criticism over sharing and publicising crime data were noted as a challenge within the COMPASS project (Boba et al, 2009, p.31).

In addition to the challenges, there were also a range of factors that were found to enable information sharing within the literature (Figure 2.3). A number of these were cited by several collaborative ventures to be critical to their establishment or continuity, whilst others may be relevant for consideration in the economic crime capacity.

Figure 2.3: Summary of key enablers identified in information sharing schemes



An important element of any collaborative scheme, and one closely linked to the success or failure of a project, is that of its governance structure. Just as this was identified as one of the challenges faced by DELJIS, a functioning governance structure is critical to success (Canestraro et al, 2009, p.125). The governing board should be inclusive and representative of participating parties (Fedorowicz et al, 2007, p.804; Gil-Garcia et al, 2005, p.7) and there should be clear lines of authority and accountability in place (Schooley & Horan, 2007, p.780). It is also widely recognised that participants should have belief in the project, and have a shared

vision and collective appreciation of the purpose and value of information sharing (Bharosa et al, 2010, p.58; Barker, 2012, p.21; Canestraro et al, 2009; p.122; Li & Lin, 2006, p.1653). To this end, it is important for participants to harmonise their organisational goals with the purpose of the collaboration (Fedorowicz et al, 2007, p.803; Schooley & Horan, 2007, p.780; Zheng et al, 2008, p.96). Promoting greater mutual understanding of each other's operations and information needs can enable more effective information sharing (Bharosa et al, 2010, p.59), whilst fostering trust is also essential if the collaboration is to work (Canestraro et al, 2009, p.125; Li & Lin, 2006, p.1650; Luna-Reyes et al, 2007, p.813). Many of the projects found that establishing data sharing agreements was an important early activity, albeit a time-consuming one (Chen et al, 2004, p.339; Fedorowicz et al, 2007, p.803; Schooley & Horan, 2007, p.773). Depending upon the context, agreements may cover such issues as protocols for secure exchange of information (Chen et al, 2004, p.337) as well as agreements over costs and over the ownership of shared information (Fedorowicz et al, 2007, p.803; Gil-Garcia et al, 2005, p.7) amongst other matters. Where contextually possible to do so, harmonising processes across agencies was found to be beneficial toward effective collaboration (Zheng et al, 2008, p.96), as was promoting shared norms, standards and values within participant agencies to foster a culture that embraced the sharing of information (Bharosa et al, 2010, p.60). Cultivating norms for information sharing will influence the attitudes of employees, and widely shared attitudes can influence and change group culture (Clements & Jones, 2008, p.71).

Strong leadership and senior level support was also integral to the success of many of the programmes (Canestraro et al, 2009, p.125; Gil-Garcia et al, 2005, p.7; Li & Lin, 2006, p.1653; Luna-Reyes et al, 2007; p.818; Zheng et al, 2008, p.95), whilst the personal relationship between agency leaders was also noted as being a contributory factor to success in one instance (Yang et al, 2012, p.S57). DELJIS found that securing a partnership with a state police body was a critical achievement as this became a gateway that encouraged other law enforcement bodies to co-operate (Gil-Garcia et al, 2005, p.7).

The roles and relationships between participants was also, unsurprisingly, an important factor in the success of information sharing schemes. Establishing clear roles and responsibilities is important (Canestraro et al, 2009, p.125), as is having regular meetings between participants (Schooley & Horan, 2007, p.776). The JNET project discovered that allowing agencies to determine their own levels of

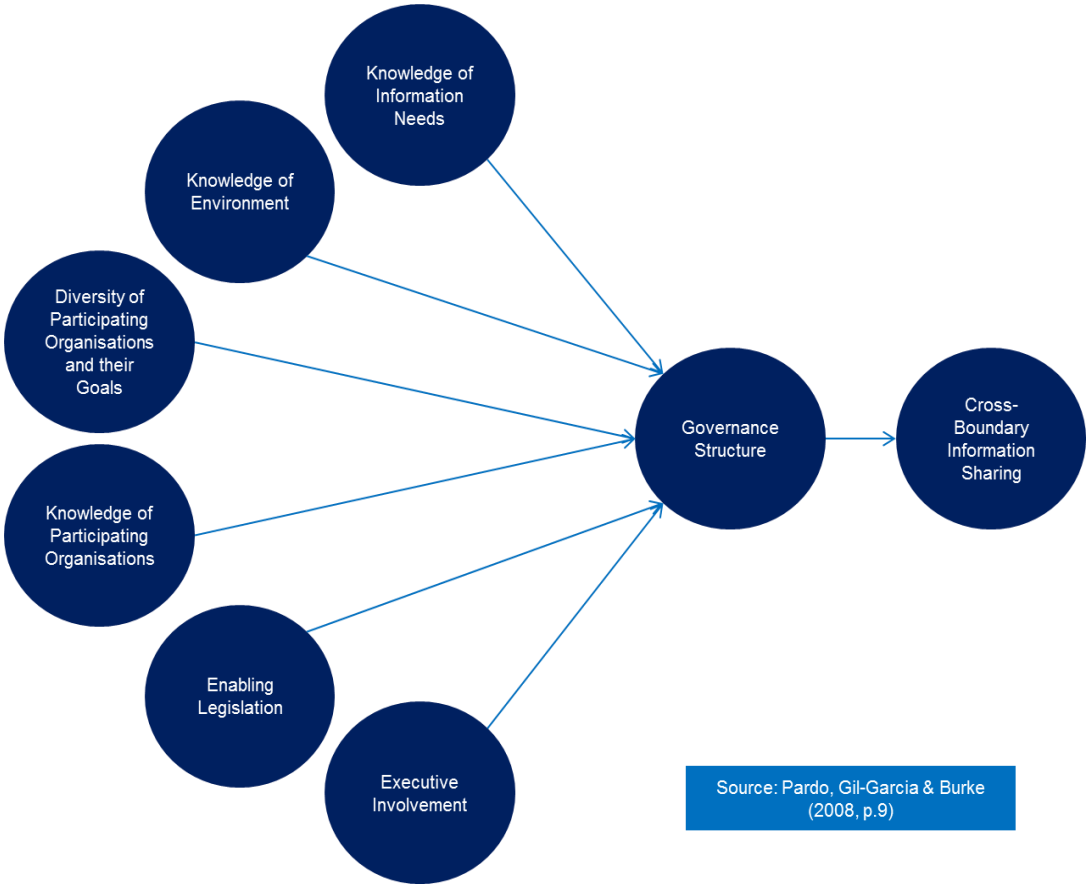
participation encouraged continuing involvement (Gil-Garcia et al, 2005, p.7), although differing levels of participation could potentially be problematic in some instances. Establishing problem-solving committees and having a dedicated project team was found to be beneficial in one project (Boba et al, 2009, pp.30-32), whilst another emphasised the importance of having a network of decision makers capable of changing the institutional environment where managers within participating organisations couldn't resolve issues (Luna-Reyes et al, 2007, p.822).

Care in the design of information sharing systems and interfaces can be integral to the success of information sharing schemes, and can help to overcome other barriers to successful collaboration, such as lack of trust and unwillingness to share (Chau, Atabakhsh, Zeng & Chen, 2001; Chen et al, 2002; Gottschalk, 2005, p.619; Zeng et al, 2003; Zhao et al, 2006, pp.625-631). Allowing visualisation of outputs can assist users to handle complex data sets (Chen et al, 2004, p.337). Involving staff during the design of the project, and providing adequate training to them, can also assist in the successful implementation of the projects (Gil-Garcia et al, 2005, p.7).

The collaborative schemes examined above demonstrate that, despite the complexities involved in information sharing in both anti-crime and non-law enforcement contexts, it is possible to achieve, even on a large scale involving many participants. This notwithstanding, each project had to overcome numerous barriers, but their success demonstrates that it can be done. Several factors contributing to their success have been identified, including the importance both of effective leadership and maintaining relationships with clear lines of responsibility and communication, and ensuring that participating organisations understand each other's needs and align their commitment to information sharing with their own organisational goals.

Another important factor that these cases demonstrated is the importance of appropriate governance structures to support effective information sharing networks. To this end, Pardo, Gil-Garcia and Burke (2008, pp.6-9) identified six elements influencing governance structures to enable cross-boundary and inter-agency information sharing. These are summarised in Figure 2.4.

Figure 2.4: Determinants of governance structures in cross-boundary information sharing initiatives



Information Sharing and Fraud

The rise of the internet and information technologies in leading governments, businesses and consumers to manage their affairs online, and the consequent migration of criminals online where they can reach a wider victim pool, maintain their anonymity and ignore physical and territorial boundaries, entails that multi-agency collaboration is more likely to be needed to combat fraud than most other types of crime (Doig & Levi, 2009, p.205). Equally, changing technologies and consumer habits have transformed how people perceive, access and consume entertainment media, with much of this being sourced and delivered online, meaning that similar approaches and collaboration is required to combat IP crime. The centrality of information and intelligence sharing to efforts against fraud were reflected in the prominence given to the issue in the Fraud Review (Fraud Review Team, 2006b), which devoted an entire chapter to the issue and made seven related recommendations, all of which the government agreed to implement (Button, Johnston & Frimpong, 2008, p.242). The NFSA, subsequently rebadged as the NFA, set up following the Fraud Review, committed itself to working to improve pan-agency

and cross-sector information sharing, and placed this at the heart of the national fraud strategy (NFSA, 2009, pp.37-39; NFA, 2011a, pp.6-7; NFA, 2011b, p.9) although, as observed in Chapter One, the agency has since been abolished. In line with this broader strategy, the government continues to build information sharing infrastructure, such as the NFIB and the Economic Crime Coordination Board, and cross-agency data sharing is central to the plans of the NCA (City of London Police, 2010; Home Office 2011, p.21; NFA, 2011a, p.9). The cross-sector aspect of anti-fraud information sharing is especially important as, unlike many types of crime, economic crime investigation is not restricted to public sector or law enforcement agencies. A significant number of organisations conduct fraud enquiries in the UK (Button, 2011, pp.251-252); there are more non-police fraud investigators than there are within the police (Doig & Levi, 2009, p.200; Levi, 2010, p.345). These anti-fraud practitioners are spread amongst public sector agencies, law firms, accountancy practices, financial services companies and other organisations, resulting in a complex and diverse spread of entities both seeking and holding information that will be of use to others to counteract economic crime threats.

It is, therefore, clear that information sharing is both desirable and necessary to effectively respond to the threat that economic crime, and its perpetrators, pose to society. However, that the matter is still the focus of many political and commercial initiatives indicate that it is not as widespread or effective as it could be. The complications are many, especially given the tensions between data protection and data sharing (6, Raab & Bellamy, 2005, p.113; Bellamy et al, 2005a, p.394; Cabinet Office, 2008, pp.11-12; Sarathy & Muralidhar, 2006, p.218; Yang & Maxwell, 2011, p.165), problems exacerbated by public concerns and political sensitivity over data security (6 et al, 2005, p.112; Fraud Review Team, 2006b, p.94; Performance and Innovation Unit [PIU], 2002, p.55), and the complexities arising from the sheer number of stakeholders across all sectors. Such tensions are not restricted to the economic crime field; governmental efforts to promote information sharing to combat terrorism have also been opposed in some quarters over privacy concerns (Smith, Seligman & Swarup, 2008, p.54). However, these complications do not account fully for the limited scope of anti-fraud information sharing that exists in the UK.

Barriers to Economic Crime Information Sharing

Despite the drivers for organisations to share anti-fraud information, and the current legal channels that enable it, there remain many challenges and barriers that prevent it from being achieved widely and effectively. Many of these are parallel to issues

that we have seen affecting information sharing in other sectors. There are many different barriers which can be analysed in different ways, but for an initial view the classification system of technical, political and organisational barriers as used by Dawes (1996, p.378) shall be followed. Other classifications have been proposed (see Figure 2.1) but this delineation remains both pertinent and succinct, and provides a useful framework for consideration of the challenges faced in information sharing.

There are a range of technical barriers that have impeded initiatives to share economic crime information between, and sometimes within, organisations. Some of the most historically challenging, widespread and most commonly discussed technical problems encountered relate to IT systems and software used to capture, store, organise, interpret, interrogate, retrieve and share information. The wide variety of solutions used, and inherent incompatibilities between them, provide significant challenges to organisations seeking to collaborate (Bellamy et al, 2005a, p.397; Fraud Review Team, 2006b, p.107; Levi & Wall, 2004, p.215). Such problems still exist although, in recent years, advances in technology have resulted in technological solutions that can overcome these challenges (Fraud Review Team, 2006b, p.107). Furthermore, utilisation of open data and technology standards, such as XML, has proven to be beneficial in the design and implementation of information sharing systems (Bajaj & Ram, 2007, pp.31-32; Luna-Reyes, Gil-Garcia & Cruz, 2007, p.814). In recognition of this, technical barriers may pose less of a challenge for information sharing than other types of barrier (Yang & Maxwell, 2011, p.169). However, while solutions do exist it would be premature to disregard such problems: utilising the available solutions would require significant investment by organisations seeking to engage in data sharing. To this extent, part of the technical challenge has arguably been superseded by a financial barrier. The financial stakes can be high: it has been noted that technology projects for the purposes of enabling information sharing can be both highly complex and, sometimes, apt to fail, making capability assessments essential prior to investment in such ventures (Cresswell, Pardo, Canestraro & Dawes, 2005, p.2; Cresswell, Pardo & Hassan, 2007, p.122). Other technical problems do exist, however. Issues such as the security of information shared remain (Cooper, 2005, p.352), as do those of data quality and reliability (NFA, 2010b, p.7), as well as complexities around data ownership and consent in some circumstances (Thomas & Walport, 2008, pp.31-35). Related to the issue of data quality is that of interpretation. Miranda and Saunders (2003, p.87) point out that most research implicitly assumes that information sharing involves the dissemination of information that has the same meaning to everyone, yet this would be a dangerous

assumption. Furthermore, in the wake of the September 11 attacks, the National Commission on Terrorist Attacks Upon the United States [9/11 Commission] highlighted another weakness, criticising intelligence systems for being based upon the assumption that it is possible to know who will want or need the information (9/11 Commission, 2004, p.417). It does not require a great stretch of the imagination to consider that such weaknesses may extend to systems designed for the sharing of economic crime information.

Technology, therefore, presents both barriers and solutions to information sharing. On the positive side, it creates new opportunities for collaboration, and can help to facilitate information sharing (Jarvenpaa & Staples, 2001, p.152). Historically, technology has also presented many barriers, some of which endure and will require significant effort, and resources, to overcome. Even where technology can help provide solutions, additional technical problems may remain. Furthermore, where technological solutions are implemented, this will only be a part of the answer. As Brazelton and Gorry (2003, p.24) observe, the technology does not create a community, and people (and organisations) will still require incentives to engage in information sharing activities.

Political barriers generally concern issues of political leadership and support for information sharing issues – often in reaction to the fallout from intelligence sharing failures as identified above, tempered by the public appetite for information protection and privacy – and to the infrastructure for information sharing and the legal framework underpinning it. According to Kennedy (2007, pp.373-377), the Human Rights Act 1998, the DPA, the common law duty of confidentiality and the restrictions upon statutory bodies to act within the confines of their *vires* all constitute obstacles to information sharing. The Freedom of Information Act 2000 has also been identified as a barrier in that it discourages private sector organisations from sharing information with public sector agencies for fear that it may subsequently be disclosed under the Act (Fraud Review Team 2006b, p.124).

The DPA is perhaps the most commonly discussed and controversial legislation in respect of information sharing. Whilst it provides exemptions to allow information sharing as detailed earlier, it is commonly misunderstood (Fraud Review Team 2006b, p.100). Both public (PIU, 2002, p.105) and private sector organisations (Fraud Review Team, 2006a, p.124) perceive that it has been used as an excuse not to share information, perhaps especially by the public sector. By way of example as

to how the DPA has been misapplied to the detriment of crime prevention, the Act was cited by Humberside Police to justify the destruction of documents relating to Soham murderer Ian Huntley (Bichard, 2004, p.127; Moss & Pease, 2004, p.7). As we have seen though, the Act does not prevent the sharing of data, but places restrictions and conditions upon it (Brooks et al, 2003, p.9); much of the problem is how the Act has been interpreted by organisations wary of being penalised under it. Having stated this, there are issues that arise from provisions of the Act, such as the 2nd Data Protection Principle which provides that data should only be used for the purposes for which it was collected (ICO, 2001, p.24) which has been vigorously upheld by successive Information Commissioners (Bellamy et al, 2005b, p.58). In practice, the 2nd Principle does not necessarily preclude large scale data sharing, and neither do political sensitivities; the UK's national data matching exercise, the National Fraud Initiative [NFI], has never faced political opposition (Bellamy et al, 2005b, p.57).

Overall, improvements to legislation and regulation alone will not provide a complete solution to enable better information sharing, as this will only tackle problems around the legal channels rather than the more subtle social regulation that occurs (6 et al, 2006, p.432); a point amply demonstrated through the limited extent of sharing taking place under the legal channels that currently enable it.

Organisational factors represent arguably the most challenging barriers impeding inter-organisational information sharing. The problems are largely cultural in nature, and are not restricted to either the anti-fraud arena or the UK: the 9/11 Commission (2004, p.416) suggested that human resistance to sharing information presented the single most significant impediment. Organisational culture is defined by Jarvenpaa and Staples (2001, p.156) as the shared values and attitudes held and espoused by members of an organisation, and these tend to be long-held and entrenched. Cultural reluctance to sharing information with other organisations is seen in both public and private sectors (Boba, Weisburd & Meeker, 2009, p.34; Grabiner, 2000, p.26; Moss and Pease, 2004, p.7; Thomas and Walport, 2008, pp.46-48).

Organisational self-interest overriding incentives to act in the greater good has been long identified as a challenge to collaboration (Dawes, 1996, p.380, Doig & Levi, 2009, p.211) in both public and private sectors. In the public sector, both HMRC and the DWP initially declined to join CIFAS – a financial services sector information sharing scheme, and a designated SAFO under the Serious Crime Act 2007 – on the

grounds that they could not recognise a benefit to themselves (NFA, 2010a, pp.13-17). Despite initiatives such as CIFAS, financial services organisations themselves have been identified as reluctant to share information with others (NFA, 2010b, pp.9-10). Competition between organisations can undermine efforts and incentives to collaborate (Aisopos et al, 2009, p.190). The silo working mentality can also be a significant barrier to engagement in information sharing (Gil-Garcia, Chun & Janssen, 2009, p.3; Gil-Garcia, Schneider, Pardo & Cresswell, 2005, p.1). Cross-sector sharing can also be undermined simply by differences in the goals, priorities and responsibilities of public and private sector organisations (Levi & Wall, 2004, p.208), and their different roles have implications for public trust in these organisations' abilities to safeguard their information (Bélanger & Carter, 2008, p.173). Information asymmetry can also be a factor, where different organisations have access to, and control over, different amounts of information to others. Information asymmetry can occur over both horizontal (where information is spread across numerous organisations and none hold the full set) and vertical (where organisations can be considered *information rich* and *information poor*) dimensions and can affect the effectiveness of information sharing, depending upon the level of involvement between stakeholders (Clarkson, Jacobsen & Batcheller, 2007, pp.828-830).

Organisational issues, including cultural impediments, are diverse and may represent the most significant obstacle to improving inter-organisational information sharing, and these problems will continue to arise even if and when the technical and political obstacles have been largely addressed. Overall, the challenges faced in improving the UK's anti-fraud information sharing environment are formidable.

Successful Anti-Fraud Information Sharing Schemes

Despite all of the challenges to anti-fraud information and intelligence sharing, some schemes have been successful and these can provide useful examples of how such collaborations may work. These vary in scope, starting with the simple agreement of common standards, as has been done for electronic passport photographs between the Identity and Passport Service [IPS] and the Driver and Vehicle Licensing Agency [DVLA] which allows the agencies to share individuals' photos for processing (Coleman, 2008, p.22; Yiu, 2012, p.13). More complex and sophisticated public sector models have also been developed, including the NFIB and Action Fraud (Magee, 2008, p.8).

A long-established and successful UK project is the NFI; a data matching scheme for identifying potential fraud. It involves the collection and matching of data from over 1,300 participating organisations, most of which are public sector. Data from participants relating to employment, taxation, residence and benefits is collected centrally and cross-referenced across the entire data set; details of matches which may indicate potential fraud are returned to the providing organisation for further investigation (Audit Commission, 2014, pp.8-9). The exercise is run biennially by the Cabinet Office (previously by the Audit Commission before its abolition) utilising powers under the Local Audit and Accountability Act 2014. While the NFI itself does not identify fraud outright, but rather returns matches that indicate potential risk back to participating bodies (Doig, 2006, pp.162-163), it has been used to identify fraud and overpayments to the collective value of £1.39 billion since inception in 1996 (Cabinet Office, 2016, p.5). Concerns have been raised about data protection and privacy issues, as the NFI involves the processing of many people's personal data with no prior, or subsequent, suspicion of fraud having been raised (Smith et el, 2011, pp.111-112), but the scheme continues unabated.

Private sector schemes such as CIFAS have been highly successful (Fraud Review Team, 2006a, p.126; Smith, Button, Johnston & Frimpong, 2011, p.73), as has the IFB, the latter cited by the Cabinet Office (2011a, p.10) as a model that should be adopted by public sector agencies.

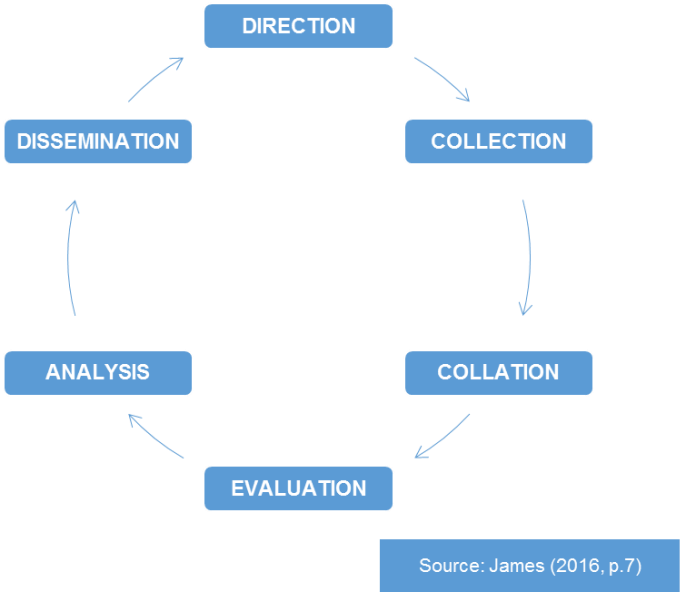
Intelligence Theory

Finally, in a study examining the professional use and dissemination of intelligence, it is worth briefly examining key theoretical aspects of intelligence handling. To this end, this section looks briefly at two important models relevant to this area: the intelligence cycle and the NIM.

The Intelligence Cycle

The intelligence cycle (Figure 2.5) has been a long-standing model within intelligence theory. It was originally developed in respect of military intelligence, but has had far wider application. The model seeks to situate each of the key stages within the generation and delivery of intelligence within a cyclical process. Despite the neatness of the model as a theoretical depiction, Johnson (2003, p.2) points out that, in reality, rather than being a neat sequence of stages, intelligence generation is more of a complex set of interactions between intelligence producers and those that task and consume it.

Figure 2.5: The intelligence cycle



Despite being the predominant theoretical model for decades it has, in recent years, been subject to scrutiny and criticism as bearing little resemblance to actual intelligence practice (Phythian, 2013, p.1). Critics, led by Hulnick (2006, pp.960-964), argue that the model fails at each stage, although much of this criticism refers to the military and political perspectives of intelligence, alongside additional concerns that that model is outdated in the world of digitised and cyber-intelligence (Warner, 2013, p.19). Due to mounting criticism of the model, various alternatives have been proposed, from a multidirectional core functions model of Direction – Collection – Processing – Dissemination, within which feedback and discussion occur between each stage (Davies, Gustafson & Rigdon, 2013, p.67) to more complex hub-and-spoke (Evans, 2009, pp.40-42) and intelligence web (Gill & Phythian, 2013, pp.30-33) models.

Despite the criticism, however, the intelligence cycle remains the main theoretical framework underlying intelligence work (Evans, 2009, p.26), and even Hulnick (2013, p.152) admits that it remains relevant in some situations and should not be discarded. Furthermore, it has been defended as the most appropriate model in the sphere of corporate intelligence in which the relationships between intelligence provider and consumer are different to those in political or military contexts (Strachan-Morris, 2013, pp.119-122). This may well also be true in the economic crime arena where the

consumer of intelligence will likely be a specialist decision maker within an organisation's anti-fraud division and closer to the producers of the intelligence.

The National Intelligence Model

The NIM is a framework developed by, and for, UK law enforcement promoting a focus on intelligence development, handling and dissemination. NIM itself developed out of the concept of intelligence-led policing [ILP], which was an approach to policing emphasising activity based on intelligence and the direction of resources towards the most serious criminals (Brady, 2008, p.106). This was part of a programme of policing reform following a series of scandals, and in the wake of influential reports from the Audit Commission and Her Majesty's Inspectorate of Constabulary [HMIC] in the 1990s calling for an intelligence-led approach (Maguire, 2000, p.317; Ratcliffe, 2002, p.54). HMIC (1997, p.11) had called for a multi-agency approach targeting and disrupting criminals through sharing intelligence and information and co-ordinating action (HMIC, 1997, p.11). However, this aim was complicated due to the number of agencies involved in UK law enforcement sector, including dozens of police forces, Customs, the Serious Fraud Office [SFO], British Transport Police and Ministry of Defence Police, amongst others (Sheptycki, 2004, p.312). These invariably had different approaches and systems for intelligence handling, such as Customs' three-tier system (of strategic, tactical and operational intelligence) and the two-tier (strategic and operational) approach of the National Crime Squad, each using different definitions of these (Sheptycki, 2004, p.326). The NIM was identified as the solution to these and other problems, by providing uniform procedures and systems, a common vocabulary, and enabling sharing (Kirby & McPherson, 2004, pp.45-46). Standardisation of processes and outputs was one of the primary purposes of the NIM (John and Maguire, 2004a, p.28).

At the time of NIM's introduction by the National Criminal Intelligence Service [NCIS] in 2000, Maguire (2000, p.316) suggests that most police forces would have claimed to be committed to sharing intelligence and to be following an ILP approach. Heaton (2000, p.351) contends that, in reality, systematic application of intelligence was a relatively new phenomenon amongst law enforcement agencies. NIM was a business model designed to change the approach to policing from a reactive service to a more proactive and collaborative one (Association of Chief Police Officers [ACPO], 2005, p.12); an attempt to professionalise law enforcement by providing a common platform and basis for decision making (Kleiven, 2007, p.257). All police forces in England and Wales were required to be NIM-compliant by April 2004 (Maguire & John, 2006,

p.69). The NIM set out a structure and procedures for the collection, storage and analysis of intelligence, a prescribed meeting structure to support decision making (Cope, 2004, p.191) and a framework to allow collaboration between agencies to share information and identify issues (Kirby & McPherson, 2004, p.46). NIM was designed to operate at three levels of policing: local, cross-jurisdictional, and serious and organised crime (nationally or internationally) (NCIS, 2000, p.8). It established four main intelligence product outputs: strategic assessments; tactical assessments, problem profiles and target profiles (Kleiven, 2007, p.259), and placed regular tasking and coordination meetings at the heart of the model, in which decisions would be made for allocation of resources based on intelligence assessments and on the direction of further development of intelligence (John & Maguire, 2004b, p.3).

While ILP and the NIM, and their proponents, promised a fundamental change to the policing model, in reality their impact was restricted by a number of challenges. The most significant of these were police resistance to change (James, 2013, p.127) and perceptions that NIM promoted a unidirectional flow of information through focus on collection of intelligence but not of its wider dissemination (Kleiven, 2007, p.270). The potential offered by the model for collaboration and partnership was hampered in the early years due to few tasking and coordination meetings, at which decisions were made, involving partner agencies (Maguire & John, 2006, p.81). The model has since been substantially revised and restructured, to the extent that the original 135 standards set out within it have been reduced to just four broad requirements: having governance and command structures; the collection and use of information and intelligence; the incorporation of knowledge management; and adherence to the tasking and coordination process (James, 2016, pp.78-79). Despite its impact being more limited than originally hoped, James (2013, p.199) suggests that NIM will continue, and praised the NCA for committing to it, which its precursor agency, SOCA, did not.

Conclusions

Information sharing is a highly relevant, and essential, strategy for effective long term action against economic crime. Given the scale and complexities of the problem, the limitless pool of victims, and the number of organisations across all sectors that are involved in the prevention and investigation of fraud, increasing information sharing is imperative if the problem is to be managed and mitigated. It is clear, however, that there are many challenges and barriers to improving and increasing such collaboration. Over recent years, a number of intelligence sharing failures and

tragedies – relating both to fraud and other types of crime – appears to have increased the appetite of politicians and the public for greater information sharing, although there is a remaining tension with privacy considerations.

The literature pertaining to information sharing in the economic crime, law enforcement, organisational and governmental contexts indicates that the challenges faced from the anti-fraud perspective have many parallels with other environments. There are extensive challenges, and while these are often considered within different frameworks many overlap, and many can be overcome.

While technological issues have historically provided significant challenges to information sharing, recent advances have ensured that most of these could be overcome, although the ability and appetite of organisations to adopt and finance the solutions remains a considerable issue. However, it is becoming increasingly recognised that many of the technical and technological challenges that have hitherto impeded information sharing are considered to be of lesser importance and magnitude to some of the other issues that must be overcome. While there is an increasing political appetite and impetus for information sharing, many political and legislative issues remain, not least of which is data protection law.

The most challenging and enduring range of issues, however, may be the organisational and cultural impediments to information sharing. These problems are varied and often deep-rooted, but are crucial to improving collaboration. Even when there is a sound infrastructure and clear legal channels in place to enable information sharing, these will continue to be underused unless and until stakeholders work to overturn these cultural constraints upon information sharing. In the meantime, those perpetrating economic crime will continue to benefit.

Some successful anti-economic crime information sharing schemes have been established. In the short term, they remain the exceptions to the rule, but offer proof of concept that the challenges can be overcome. This study will seek to fill the gap in understanding how the many impediments to information sharing can be overcome by examining how successful collaborators have tackled them. With appropriate will, resources and effort, the barriers impeding information sharing can be overcome (Zheng, Yang, Pardo & Jiang, 2009, p.9). This study will examine how this can be done to better combat economic crime, and Chapter Three will outline the approach taken to achieving this.

Chapter Three

Methodology

Introduction

As set out in previous chapters, the aim of this study is to examine both the nature of the challenges that impede effective information sharing and strategies that can overcome these. This chapter outlines the methodology employed in order to achieve these objectives. This commences with a short analysis of the underlying philosophical standpoint, which has inevitably informed the strategy. After this, the approach taken to the literature review is outlined, followed by a summary of the decisions made in the selection of methods and a discussion of the ethical issues in the research design. This is followed by an account of the design and implementation of the two phases of data collection and a discussion of the strategy employed to the management and analysis of data collected. The chapter closes with a short reflective assessment of the methods employed.

Philosophical Standpoint

The approach to research design is closely related to the researcher's philosophical standpoint, with decisions influenced by ontological and epistemological perspective (Dunne, Pryor & Yates, 2005, p.14). Therefore the philosophical perspective of the researcher will underpin the methodological choices made and may be considered the basis upon which social research is constructed (Denscombe, 2010, p.117; Grix, 2010, p.57). As noted by Creswell (2009, p.5), research practice is influenced by underlying philosophical ideas even when these notions remain in the background.

From an ontological perspective, where ontology determines how we define and understand the nature of the world (O'Leary, 2007, p.180) and how we attribute meaning to the elements that comprise reality (Crotty, 1998, pp.10-12), this study was founded on a leaning towards the constructionist perspective. Within the social science context, Bryman (2012, p.32) defines constructionism as the understanding of entities as social constructions, as opposed to objective entities in their own right (Denscombe, 2010, p.119).

Epistemologically, there are competing orthodoxies for how we come to have knowledge of the world (O'Leary, 2007, pp.76-77) and the conditions for knowledge

(Hughes & Sharrock, 1997, p.5). Some of the primary traditions within social research – the positivist and interpretivist conventions – have been argued to be wholly divergent and incompatible dichotomies. However, on the basis of underlying sympathies with elements of each of these, and in agreement with Gorard (2003, pp.9-10) who rejects use of the term 'paradigm' within this context, this research is founded on a pragmatic platform. As pragmatism is a philosophical standpoint grounded in the real world application of knowledge, it is a natural path for researching issues relating to the professional realm. Rather than being a rejection of positivism or interpretivism, it is an acceptance of the utility of both and of quantitative and qualitative methods. Pragmatism allowed the approach to research strategy to be guided solely by the research questions and the adoption of methods that would yield appropriate data to answer these, rather than placing methodological constraints upon the methods to be employed.

Literature Review

The first stage of the project, once the topic had been determined and the proposal approved, was to conduct a literature review. This was performed to survey the literature germane to the research topic (Robson, 2011 p.51, Wakefield, 2011, p.79) and to provide a contextual backdrop and rationale for the work (Denscombe, 2010, pp.29-30). A narrative review, which Bryman (2012, p.111) argues to be suitable for interpretive qualitative research, was undertaken rather than a systematic one as the research was to be inductive rather than deductive in nature. The review was conducted to provide the foundations on which the research was to be constructed (Hart, 1998, pp.26-27) and set out the theoretical backdrop against which the findings of the research would be set and developed.

There is limited academic literature directly concerned with anti-fraud and IP crime information and intelligence sharing. A body of relevant grey literature, such as government reports, was available on the subject, however. This notwithstanding, there was a corpus of literature on information sharing in other fields, including approaches to information sharing and collaboration between organisations operating in both the criminal justice and other sectors. It was around these, along with a core of key authors – the “essential and always quoted works” (Trafford & Leshem, 2008, p.71) - that the search was built, expanding on key works previously identified and broadening this out to examine a body of literature relating to information sharing schemes in the criminal justice arena. The search was then extended to other examples of collaboration, including literature around collaboration between

governments and other reactive and responsive services ranging from emergency services to disease control. This was supplemented in the initial search by a review of literature relating to knowledge management and transfer, as these were topics referenced in some of the resulting material and provided relevant insights into issues related to the subject matter.

Engaging with the literature is an iterative and ongoing process (Denscombe, 2010, pp.32-33; Wakefield, 2011, p.94). Additional literature was examined throughout the course of the research relating to ancillary issues that arose after the preliminary review had been undertaken. An example of this was literature pertaining to the NIM, which had not had not been anticipated as forming such a central topic until data collection was underway. As such, the approach to the literature taken throughout the research was intended to be flexible and responsive to issues arising from the data collected.

Research Strategy

The research strategy and the methods employed were primarily driven by the nature of the research questions themselves, as noted in Chapter One. Creswell (2009, p.18) cites numerous factors, including the background, experience and worldview of the researcher, the research problem, strategy, methods and the audience, as influencing research design. Being philosophically unbound to either qualitative or quantitative research paradigms, a variety of methodological approaches were possible for the research. As the research was undertaken primarily towards a doctoral thesis the immediate audience in terms of academic examiners was well understood, although it was still undertaken with a longer term aim of publishing more widely and with a view to using the findings towards more practical application in the anti-fraud field.

The research questions themselves were framed as exploratory lines of enquiry, looking to examine the nature of the challenges to effective information sharing, and the strategies that are employed by some organisations to overcome these. The questions called for descriptive data in order to distinguish the essential characteristics of approaches to collaboration, and to examine patterns and parallels between these (Semmens, 2011, p.56). The exploratory nature of the research is appropriate as it seeks to assist the development of understanding in an area to which there is no extensive body of extant theory, and to explore this field of enquiry (Denscombe, 2010, p.105). Given the limited extent of previous research, the

complexity of the subject matter and the exploratory nature of the questions which would be difficult to answer with numerical data, it was considered appropriate to adopt a research strategy focused on qualitative data (Frankel & Devers, 2000, p.253). The adoption of a flexible design strategy was appropriate to allow development of research instruments as the research progressed with less pre-specification required (Robson, 2011, p.74; Semmens, 2011, p.58).

While broadly convinced that a research design focussed on collecting qualitative data would be appropriate, consideration was given to the possibility of employing a mixed methods strategy to collect, analyse and interpret both quantitative and qualitative data in respect of some of the research questions (Creswell & Tashakkori, 2007, p.303). Proponents of mixed methods research point to several advantages, including triangulation of data to enhance validity of findings (Robson, 2011, p.158) or to better understand social reality by investigating it from different angles (Bachman & Schutt, 2007, pp.351-352). For some, mixed methods research is not just the combination or synthesis of paradigms but rather presents a third way (Johnson, Onwuegbuzie & Turner, 2007, p.129). Some argue that this can help to overcome identified weaknesses arising from employing purely qualitative or quantitative designs (Johnson & Onwuegbuzie, 2004, pp.19-20). Not all agree, however. Sale, Lohfeld and Brazil (2002, p.50) contend that, rather than mitigating the weaknesses of either paradigm, combining methods from different paradigmatic camps risks devaluing both, and that either is capable of producing results that should not require validation from other methods. Whilst due consideration was given to these arguments, the final decision was made by going back to the research questions, determining that these would not be answered better with the inclusion of quantitative data, nor would this likely help validate the findings. Once a strategy of seeking qualitative data was elected, this did not preclude the consideration of employing multiple methods towards this end. Whilst some writers restrict the definition of mixed methods research to obtaining both quantitative and qualitative data (Bryman, 2012, p.628; Johnson & Onwuegbuzie, 2014, p.42; Johnson, Onwuegbuzie & Turner, 2007, p.129), others, such as Yin (2006, p.42), argue that a broader range of potential mixes can occur when the focus is removed from the divergent paradigms altogether, and that mixed methods research can encapsulate multiple methods that seek to collect and use similar types of data.

Having reflected carefully upon the research questions, giving due consideration to the depth of descriptive data that would be needed to answer them, a two-phase data

collection strategy was devised. This strategy was designed to afford the best opportunity to collect data from a wide range of sources as well as detailed information about organisational approaches and strategies to information and intelligence sharing. This approach could fall within the definition of mixed methods research as described by Yin (2006, p.42.), or be defined as a multi-methods strategy as both methods were geared towards collection of qualitative data. The first phase would comprise a case study review of an organisation actively involved in intelligence sharing with other entities for the purposes of fighting economic crime. The intention of pursuing a case study design was to gather a body of data about the strategies and approaches employed by the organisation examined to a greater level of detail than would be afforded by many other methods, such as a survey or single interview. For the second phase of the data collection, the scope of the research would be broadened by collecting additional data from other organisations involved in, or closely concerned with, anti-fraud information sharing. This was to be achieved by conducting a series of semi-structured research interviews with relevant parties.

Alternative methods were considered, but were rejected as these did not seem as suitable to collect the type of data needed to best answer the research questions. Quantitative instruments, such as surveys or structured interviews, could have been employed targeting a wide range of organisations and professionals engaged in anti-fraud work and collaboration. However, this was not considered to be an adequate strategy as the research questions were exploratory in nature, whereas a quantitative survey methodology would have been better suited to deductive, rather than inductive research (Bryman, 2012, p.36, Bachman & Schutt, 2007, p.19; Creswell, 2009, p.18). Other qualitative methods were also considered, but rejected on the basis of being less suited to fully answering the research questions. For example, a design based on documentary analysis would not have been appropriate given limited documentary evidence available to provide suitable data. An ethnographic approach may have been suitable in the case study setting, but would not have been practical given that the research had to be conducted around the constraints of the researcher's full time employment.

Ethical Considerations

Ethical issues were an important consideration throughout the study, and required careful planning at the design stage. It is a fundamental principal of UK academic research that the research will be conducted ethically, with detailed consideration given to ensuring that participants will be treated with due respect (Grix, 2010, p.143;

Macfarlane, 2009, p.9). Research should be planned and conducted taking account of, and with due deference to, the wider cultural context and the accepted values and mores of the society in which it is undertaken (Brinkman & Kvale, 2005, p.162; Denscombe, 2010, pp.59-60). There are a number of ethical principles which were taken into consideration, but foremost amongst these were those of protecting participants from harm and ensuring that they were able to make informed decisions about whether or not they wished to take part.

The principle of protection from harm extends not only to the threat of physical harm but also from other risks including psychological harm, discomfort (Bryman, 2012, pp.135-136) and reputational impact (Bachman & Schutt, 2007, p.288). Denscombe (2010, pp.63-65) emphasises the need to protect the interests of research participants, which may encapsulate the above but also extends to issues such as stress, invasion of privacy, protection of identity and ensuring the confidentiality of data.

The principle of informed consent is also a significant consideration in the conduct of modern research (Denscombe, 2010, p.67, Davies & Francis, 2011, pp.283-284). However, while this is central to the ethical codes of many professional bodies, including those of the British Society of Criminology (2015, p.6) and the British Sociological Association (2002, p.3), it is not necessarily a clear-cut concept (Bryman, 2012, p.138; Dunne, Pryor & Yates, 2005, p.63; Grix, 2010, pp.145-147). As such, it was important to take steps to ensure that participants were fully cognisant of what they are being asked to consent to and the implications thereof (Davies, 2011, p.167).

Careful consideration was given to the ethical issues and questions posed by the study design. Furthermore, in line with the requirements stipulated by the University of Portsmouth's Ethics Policy (2015, p.7), formal ethical approval was sought for the research, including conducting a risk assessment and making a detailed submission to the Research Ethics Committee of ethical considerations and planned safeguards. This submission was made and revised in late 2013, and consent received in early 2014. The risk assessment is reproduced as Appendix 1, and the ethical approval notification letter as Appendix 2.

From assessment of the risks it became clear that these were more straightforward for the second phase of the research than for the case study. This appraisal by no means disregarded the ethical issues involved in research interviews; Kvale and

Brinkmann (2009, p.62) state that “ethical issues go through the entire process of an interview investigation and potential ethical concerns should be taken into consideration from the very start of an investigation to the final report”. However, as the topic of the research was not contentious and the interviews did not seek personal information from participants, did not expose them to risk of harm and involved no power issues, the overall risks were determined to be manageable. These related primarily to ensuring that participants were able to provide informed consent, and that their identities and data were protected and securely processed in line with the DPA. In order to mitigate these risks, potential participants were provided with a detailed Information Sheet outlining the nature and purpose of the research and setting out how their data would be used, stored and destroyed once the project had been completed. Participants’ identities would be protected by agreeing not to report their, or their employing organisations’, names in any output from the research. It was made clear that participation was voluntary, and that they had the right to withdraw up to the point where data had been analysed and integrated with other findings. Participants were advised that the interviews would be recorded, and were asked to provide written consent confirming that they agreed to take part, and were also asked for recorded verbal consent at the start of each recorded interview. Copies of the Invitation Letter, the Information Sheet, and the Consent Form provided to participants are reproduced in Appendices 3-5.

The same issues were relevant to the case study interviews. However, due to the nature of this phase additional risks were also assessed. Firstly, it would be necessary for the organisation that was the subject of the study to be identified within the thesis and any subsequent publications arising from it. There would also be the probability that the research would involve exposure to sensitive operational information relating to the organisation. Both of these would expose the organisation to a certain amount of risk. These risks were set out in a detailed information sheet addressed to the head of the organisation, and discussed openly with him in preliminary negotiations, and a Consent Form obtained acknowledging that the organisation agreed to take part having been notified of these risks. The information sheet also provided assurance about sensitive data not being disclosed in the output. During access negotiations, it was also agreed that use of any materials in the output that may potentially be sensitive be discussed and agreed first.

Additionally, it was recognised that the issue of power relationships (Denscombe, 2010, pp.71-72) might be relevant in that, once agreement had been obtained from

an organisation to take part in the research, members of staff may feel obliged to participate. This was addressed in the information sheets issued to both the case study organisation and to the individual staff members selected as potential participants, which established that individual consent would be sought in each instance, and that no obligation was conferred to staff members by the organisational consent. Each targeted staff member was given full details of the nature of the research and their role within it and was asked to voluntarily participate, giving them the same rights of refusal or withdrawal as given to individual interviewees in the other phase of the data collection. Furthermore, the Information Sheets made clear that while participants' names would not be disclosed in any outputs in order to protect their identities, there was an underlying risk that their identities may be inferred by people who knew that they were employed at the organisation.

In this way, the key risks were identified and addressed, mitigated as much as reasonably possible, and participants of both elements of the study were made aware of the risks of participation and the precautions taken to protect them. Copies of the Invitation Letters, Information Sheets and Consent forms used in the case study element of the research are reproduced in Appendices 6-15.

Data Collection Phase One: Case Study

Case study research was chosen for the first of the two phases of data collection. Case studies are reviews into single, or multiple, units of enquiry (Bryman, 2012, p.66; Creswell, 2009, p.13), and are a strategy that allows the researcher to gain detailed understanding of the case (Denscombe, 2007, p.36; Hagan, 1982, p.122; Noor, 2008, pp.1602-1603). Noor (2008, p.1602) observes that the case study does not aim to study the entirety of the organisation, but focuses on a particular issue or feature, and can be used towards the development of theory (Bryman, 2012, p.71; Darke, Shanks & Broadbent, 1998, p.275). Furthermore, Appleton (2002, p.87) suggests that case studies are particularly valuable when there is limited knowledge about a particular subject. As such, it is a strategy that lends itself well to the aims of the research.

As a research strategy, case studies have been subject to a number of criticisms. Flyvberg (2006, p.221) identifies five commonly cited criticisms as being:

- that practical, context-dependent knowledge is less valuable than theoretical knowledge

- that case studies may be subject to verification bias, and may serve to confirm the predetermined views of the researcher
- that case studies are better for the generation of hypotheses rather than theory
- that is it difficult to develop theory on the basis of analysis of specific cases
- that findings from a single case cannot be generalised.

For Flyvberg, each of these is misplaced. He argues that case studies are well suited to development of context-dependent knowledge, and that detailed understanding of real-world phenomena is required to elevate understanding from rudimentary rule-based insight to expert knowledge (Flyvberg, 2006, pp.221-222). The issue of researcher bias is rejected on several grounds: that such criticism is often made from the positivist standpoint that qualitative enquiry is unscientific; that verification bias is not specific to case study research; and on the evidence of many case studies where findings have discredited initial hypotheses or caused them to be amended (Flyvberg, 2006, pp.234-237). Darke et al (1998, p.286), considering bias during data collection and analysis, assert that risks may be reduced through strategies such as triangulation of data from multiple sources. The remaining criticisms cited concern whether case study findings may be generalised, and used to generate theory. Again Flyvberg (2006, pp. 224-225) points to the positivist source of this criticism, as scientists cannot generalise from a single case, a point with which Yin (2009, p.15) – one of the principal proponents of case study research – concurs. Yin (2009, p.38), however, contends that case study findings may be better suited to theoretical rather than statistical generalisation. Flyvberg (2006, pp.225-226) argues that findings may be generalisable dependent on careful case selection. Appleton (2002, p.90) takes a different view again arguing that, for constructivist research, generalisation as a concept is better amended to that of transferability, to how well findings from one case may be transferred to another. This, in turn, may help to explain the phenomenon of mimetic isomorphism, in which some organisations in uncertain environments will mimic the characteristics of others that are perceived to be successful (Williams et al, 2009, pp.17-18). This latter argument is compelling, suggesting that the findings from this research could be transferable and that organisations that are not currently engaged in, or effective at, sharing information should be able to adopt and adapt the strategies employed by others. This may accord with the viewpoint expressed by Stake (1978, p.6) who argued that case studies are perhaps most useful for increasing understanding and extending the experience of others.

The question that underlies any case study research is 'what is a case?' While space restrictions do not allow an extended examination of this, it is worth noting that there are multiple viewpoints and, in some instances, defining a case may not be a straightforward matter. A case can be many things. It can be any one of many units of analysis, such as an organisation, an individual, a group, an event or a phenomenon (Darke et al, 1998, p.280; Robson, 2011, p.135; Yin, 2012, p.6). A case could be a particular decision, an activity or strategy, or a process (Yin, 2009, p.29). Appleton (2002, pp.85-86) argues that, given the extensive range of objects and phenomena cited within the literature as potential cases, virtually anything may be determined to be the case within the right context and if adequately defined. For Bryman (2012, p.69), the case must be a discrete item of interest on which the researcher can focus on the unique characteristics. Thomas (2011, pp.14-15) extends the focus, suggesting that the case must be an example of something: a simple description of a particular object or event in itself would not constitute a case unless it was an example of a particular characteristic, such as a successful project, or a noteworthy failure. Therefore he emphasises the contextual relevance of the unit of analysis. The case also need not be the entirety of an object; if a project is based within a particular organisation, for example, the case study may focus on one particular aspect or division rather than the entity as a whole (Robson, 2011, p.138).

The case study phase of the research was conceived from the outset to be a single case design. This was based on practical considerations due to the constraints of part-time research, especially given that the case study was only one part of the data collection. While one of the commonly cited risks pertaining to a single case design include the issue of whether the findings can be generalised (Flyvberg, 2006, p.224), by having an additional phase of data collection from other sources helped mitigate the risk by allowing triangulation of the data. While an alternative would have been to conduct a multiple case design, and not conduct an additional phase of stand-alone research interviews, this would not have been appropriate for this project. There were two primary reasons for this. The first was that by restricting the sources of data to two main cases, rather than one main case and a wider range of additional sources would limit the breadth of the study, and could potentially render the findings less generalisable. Secondly, there was only a small pool of suitable potential cases to target for such a study, and there was no certainty of getting one, let alone two, to agree to be the subject of such research within a reasonable time frame.

Selection of an appropriate case for the study was, therefore, a critical decision. Purposive selection of the case was essential; random sampling would be an inappropriate strategy for a case study design as it could result in the selection of a case that may yield little suitable data. A shortlist was drawn up of organisations actively focussed on the sharing of information for anti-fraud purposes. These organisations were shortlisted because they were all examples of key cases (Thomas, 2011, p.77), or exemplary cases (Yin, 2012, p.35). Additionally, such examples could be considered to be revelatory cases (Yin 2009, pp.48-49) as no case study research had been performed into the anti-crime intelligence sharing functions of non-law enforcement organisations in the UK. First and second choices were selected, both of which operated within the insurance field, and these were contacted in turn with a view to obtaining their agreement to participate in the study.

Several attempts were made to contact these organisations, with no response being received from the first choice. Shortly after the second had been contacted, good fortune struck. A chance opportunity arose at a conference in October 2013 to speak with the Director General of FACT, an organisation devoted to tackling intellectual property crime, following a presentation given by him on FACT's intelligence-led and collaborative approach. His presentation suggested that FACT would be an ideal candidate for the case study, and a meeting was engineered with the Director General whilst he was at the conference. In this, the nature of the research and a request to use FACT as the subject of the case study were discussed, and he expressed willingness to correspond further.

In order to secure FACT's participation, further negotiations were held over several weeks, in which the nature and purpose of the research and the case study focus were discussed. The Director General provided background information about the organisation, including copies of its strategic assessment document and organisational structure to enable planning of priorities in terms of members of staff to interview.

A meeting was held with the Director General in February 2014 to make arrangements for the data collection. Preliminary agreements were reached as to when the research would take place, which staff would be invited for interview, and for the Director General to distribute information sheets and consent forms to those staff in order that they could make informed decisions as to whether or not they wished to participate. He also provided written and signed consent on behalf of FACT

for the research to take place, confirming that he was content for the organisation to be identified by name as the subject of the case study. Within a few weeks of this meeting, we had agreed the timeframe for the data collection to be conducted at FACT's office in March and April 2014.

Yin outlines six main sources of data for case study research: documents, interviews, archive records, direct observation, participant observation and artefacts (Yin, 2009, p.101), although both he and Thomas (2011, p.162) agree that additional sources may be of use. The primary method employed was the semi-structured interview. As there were just two weeks on site full time in which to undertake the fieldwork, conducting interviews provided the opportunity to gather the greatest amount of data from across different parts of the organisation within this timeframe. In addition to interview data, some documents were collected to obtain additional information, as well as some observation of meetings and day-to-day work insofar as time allowed. Due to time constraints, there was little opportunity in practice to spend time in observations, although sessions were conducted with members of both the Intelligence and the Internet Investigations teams to observe their work. Due to the limited time available for this activity, this was primarily of benefit from a contextual perspective, allowing observation of matters that were discussed during interview sessions and providing insight into how FACT worked rather than data towards the research questions. One of FACT's Tasking and Coordination meetings was observed, in which all operational staff and managers were involved and in which the status of all active investigations was discussed and objectives and priorities set relating to case work and intelligence. Documentation was collected relating to FACT's strategy, policies and procedures to allow better understanding of the framework within which it operated, as well as samples of operational documents relevant to the topic of the research, such as copies of information sharing agreements, samples of intelligence products and board papers. These were all valuable sources of additional data. However, by seeking and analysing different forms of data, the study conformed to Heidensohn's (2008, p.209) observation that most case studies employ multiple methods of data collection, which can enhance triangulation and validation within the study.

In all, during two weeks onsite fieldwork, twenty-four tape-recorded semi-structured interviews were conducted. This comprised just over 50% of FACT by capacity headcount. Some short, informal and non-recorded chats were also conducted with additional support staff. The interviews varied in length, with most falling between

forty minutes and an hour. Figure 3.1 below provides details of the formal case study interviews. One of the interviews, with a recently recruited member of staff, lasted just ten minutes, but covered issues such as her perception of the role, and the training that she had received, while the longest two interviews – with the Director General and with the Intelligence Manager – each approached two hours in length. Interviews were conducted with all senior officers, most of the Intelligence team, members of the other key teams and functions as well as a selection of support staff. This data was supplemented with a body of documentary material collected for further examination and field notes from observations of meetings and of time spent with the Intelligence and Internet Investigations teams.

Figure 3.1: Case study interviewees

Interviewee Ref.	Position
CS/01	Field Investigator
CS/02	Market Strategist
CS/03	IT Support [contractor]
CS/04	Criminal Justice Officer
CS/05	Forensics Supervisor [IT forensics]
CS/06	Internet Industry Liaison Officer [ISP liaison]
CS/07	Director of Communications
CS/08	Business Development Manager [inc. Human Resource function]
CS/09	Field Investigator
CS/10	Certification Manager
CS/11	Investigations Manager
CS/12	Intelligence Researcher
CS/13	Forensic Examiner [IT forensics]
CS/14	Internet Investigator
CS/15	Internet Investigator
CS/16	Legal Counsel
CS/17	Intelligence Analyst
CS/18	Director General
CS/19	Internet Researcher
CS/20	Internet Supervisor
CS/21	Intelligence Researcher
CS/22	Intelligence Analyst
CS/23	Director of Investigations and Intelligence
CS/24	Intelligence Manager

Data Collection Phase Two: Research Interviews

The second phase of data collection involved a series of stand-alone interviews conducted with professionals actively engaged with, or having specialist knowledge of, information sharing relating to the prevention or investigation of economic crime.

Semi-structured interviews were selected as the data collection method for this phase as these provide a framework to guide conversations but afford flexibility within interviews to respond to topics arising during conversation rather than sticking rigidly to a fixed question set (Denscombe, 2007, p.176, Kvale & Brinkmann, 2009, p.130; Robson, 2011, p.280). Interviews seek to obtain contextual accounts from the interviewee's perspective and experience (DiCicco-Bloom & Crabtree, 2006, p.319; Kvale & Brinkmann, 2009, p.3) and can provide a rich source of data that is useful for research into complex phenomena (Denscombe, 2007, p.174; Hagan, 1982, p.82).

However, there are problems with the semi-structured interview as a research instrument. They can be time consuming and expensive to conduct, transcribe and analyse (Denscombe, 2007, p.174; Hagan; 1982, p.83). Robson (2011, p.281) observes that criticism has been levelled in respect of their not producing standardised responses, thus raising questions about reliability and validity of the data. The data collected from interviews can cause problems in the analysis phase due to the volume of data that can be amassed (Bryman, 2012, p.565). Furthermore, the method has been criticised as being too susceptible to researcher subjectivity or bias (Hagan, 1982, p.83; Kvale, 1994, pp.154-159). These can be valid concerns and the issue of the volume of data will be discussed later in the chapter. Some issues, such as concerns over validity and lack of standardisation may be philosophically-based (Kvale, 1994, p.170). Measures can be taken to reduce bias, including through reflection on, and declaration of, the researcher's position (Kvale, 1994, p.155; Malterud, 2001, p.484) and through adopting a neutral stance in questions posed during interviews (Robson, 2011, p.282). Steps were taken in these respects in that neutrality was sought through careful construction, review and revision of the research instrument. The researcher's position is that of an anti-fraud practitioner who is supportive of increased information sharing and motivated by professional experience of some of the problems involved to conducting this study to better understand how it can be appropriately and legally achieved. An additional risk is that of elite bias, where the researcher seeks information only from those with a particular status, and does not obtain the full picture (Myers & Newman, 2007, p.5).

Whilst this risk is present in stand-alone interviews, it has been mitigated in two respects in terms of this research. Firstly, the sample was not selected in terms of hierarchical status. Secondly, the case study element has helped to ensure that data has been gathered from participants operating at all levels: senior, junior, operational and managerial.

Effective interviewing is subject to the skills of the researcher as an interviewer, with the quality of the data collected dependent on this ability (Kvale & Brinkmann, 2009, p.82); these are skills that require practice and, ideally, training (Robson, 2011, p.301). The researcher had previous experience of conducting semi-structured research interviews from a preliminary study earlier in the doctoral programme as well as extensive experience of conducting fact-finding interviews in a professional context.

A purposive sampling strategy was employed, recognising that careful sample selection would be critical to obtaining suitable data (Bryman, 2012, p.416; Coyne, 1997, p.623). As the research strategy was focused on interviewing subject matter experts, purposive sampling was a natural strategy to adopt in order to access information-rich sources of data (Devers & Frankel, 2000, p.264) on the basis of participants' expertise as a 'key informant sample' (Marshall, 1996, p.523). Alternative sampling strategies were rejected as being less suitable. Probability sampling would have been unlikely to have returned a sample with appropriate knowledge and expertise. Convenience sampling lacks credibility, and would also be unlikely to generate appropriate data (Marshall, 1996, p.523). While purposive sampling can be prone to bias (National Audit Office, n.d., p.11), the risk was minimised for this study as the sample demands selection of organisations known to be successfully engaged in information sharing, and the quality of the findings would be impeded if effort were not spent to select the best possible examples. Furthermore, the incorporation of snowball sampling also reduced the scope for bias.

As the strategy demanded a very specific sample of practitioners and subject matter experts, two main approaches were taken to selecting the sample. The first was to draw on the researcher's professional knowledge as to those organisations that were actively involved in, or known for, sharing intelligence for anti-fraud purposes. The second was to adopt a measure of snowball sampling, with participants from both phases suggesting additional people and organisations to engage with for the research. An initial target list was drawn up, comprising public and private sector

entities engaged in anti-fraud information sharing, and other relevant parties with insight at the strategic or policy level, such as regulators and legislators. This list was supplemented by snowball sampling recommendations made by some participants as data collection progressed.

An interview schedule was prepared to provide a framework for the meetings, although allowing flexibility in how closely this was adhered to. One main schedule was prepared before this phase of data collection commenced, although it was subsequently adjusted for a few interviews where necessary (for example, when the interviewee's organisation had a policy, rather than operational, interest in intelligence sharing). Copies of the schedules are reproduced in Appendix 17. The first interview was used as a pilot, by agreement with the participant, and was used not only to collect data but also to refine the research instrument in line with generally recommended practice (Bryman, 2012, pp.263-264; Kezar, 2000, p.393; van Teijlingen & Hundley, 2001, p.1). While it is useful to bear in mind the concern that pilot participants generally report no issues with the approach or questions, thereby limiting their effectiveness in helping to refine the research instrument (Sampson, 2004, p.395), the first interviewee had, coincidentally, engaged in research on a similar topic for his own Master's degree several years earlier, and understood the value of such feedback. Some minor revisions were made to the research instrument following completion of the pilot interview, in terms of removing and adding questions, revising the structure and emphasis, and implementing small changes to the wording.

Once the intended sample had been drawn up, potential participants were contacted through a variety of means. Some were contacted directly, using contact details researched online. Some success was had by this method, but some requests were rejected and a number of approaches received no response. In one instance, a high priority target was successfully contacted through a blind approach on LinkedIn. The most successful approach, however, other than snowball sampling where other participants generally agreed to make an introduction to the recommended party, was through exploitation of the researcher's professional network. Professional contacts in law enforcement and various industries were utilised to seek the right people to contact for the target organisations. In many instances these contacts also made direct introductions, considerably easing the process of access negotiation. Once contact had been established, usually by email followed by a telephone conversation, the participant would be sent the Information Sheet and Consent Form as described in the Ethics section above.

As with the case study interviews, the second phase interviews were audio recorded to aid retention. Suitable preparations were made regarding familiarity with the recording device, ensuring there was sufficient memory space and having a backup recorder as well as material for taking notes. A flexible approach was taken to allow for unexpected situations; two interviews involved multiple interviewees, with the original participant inviting another person to take part, while another interviewee did not wish to be recorded so contemporaneous notes were taken instead. Interviews were conducted at locations suitable for the interviewee, and steps taken to prevent background noise and interference on the recordings.

For this phase of data collection, twenty-two research interviews were conducted, involving twenty-four interviewees from nineteen different organisations across multiple sectors. Figure 3.2 provides details of these interviewees.

Figure 3.2: Non-case study interviewees

Interview No.	Interviewee Ref.	Organisation Type	Position
1	RI/01	Anti-fraud focussed professional services firm	Counter Fraud Manager
2	RI/02	Central government department	Head of Policy for Data Sharing for Fraud, Error & Debt
3	RI/03	Industry-based intelligence sharing scheme [finance/insurance sector]	Director
4	RI/04	Industry-based intelligence sharing scheme [finance/insurance sector]	Deputy Head of Financial Crime and Strategic Intelligence
5	RI/05	Insurance industry – peripheral services provider	Chief Executive Officer
6	RI/06	Industry-based intelligence sharing scheme [finance/insurance sector]	Compliance Manager
7	RI/07	Investment Bank	Vice President – Fraud Program Manager
8	RI/08	Regulator / quasi-autonomous non-governmental organisation	Head of Strategic Liaison
9	RI/09	Law enforcement agency: police	Intelligence Manager
10	RI/10	Law enforcement agency: police	Head of Debrief Team
11	RI/11	Law enforcement agency: police	Head of Intelligence
12	RI/12	Cross-sector intelligence sharing scheme	Coordinator
13	RI/13	Law enforcement agency: police	[Intelligence Lead – multiple local intelligence teams]
14	RI/14	Retail bank	Director of Investigations
15	RI/15	Industry-based intelligence sharing scheme [communications sector]	Chief Executive Officer
16	RI/16	Central government department	Researcher [fraud intelligence sharing project]
17	RI/17A RI/17B	Industry-based intelligence sharing scheme (finance/insurance sector)	Managing Director Business Development Director [previously Managing Director]
18	RI/18	Law enforcement agency: non-police	Economic Intelligence Team [lead on two intelligence sharing projects]
19	RI/19A RI/19B	Insurance company	Head of Intelligence – Claims and Investigation Intelligence Analyst
20	RI/20	Central government: executive agency	Head of Intelligence
21	RI/21	Central government: executive agency	Head of Intelligence Hub
22	RI/22	Law enforcement agency: non-police	Principal Intelligence Officer

Transcription and Analysis

Almost as soon as the data collection was underway, the task of transcribing the interview data was started. Due to the number of interviews undertaken, it was recognised that this would be a lengthy and time consuming process. However, this was done by the researcher for two reasons. Firstly, it would have been expensive to use a transcription service given the number of interviews involved. Secondly, and more importantly, the process of transcription can assist in getting to know the data (Robson, 2011, p.478. For Noaks and Wincup (2004, p.129) transcription is a valuable part of the analysis phase of research. In order to make it more manageable, the decision was taken to fully transcribe all of the second phase interviews, but just the most apposite of the case study interviews: those involving the Intelligence team and senior officers; those which provided the data most relevant to intelligence handling and sharing. This comprised nine of the twenty-four case study interviews. The remaining fifteen were coded directly from the audio recordings, focusing on the most pertinent topics arising within them. This process involved playing back each of the recordings multiple times whilst coding.

In order to assist with data management throughout coding and analysis, Computer Assisted Qualitative Data Analysis Software (CAQDAS) was used. While Robson's (2011, p.472) caution that consideration must be given to the time saving afforded by these packages against the time invested to learn how to use them was noted, the volume of data that had been collected for analysis and the functionality of such software made it a rational decision. This was taken in full knowledge that CAQDAS is a data management tool and not a replacement to the intellectual effort and decisions required to code and analyse data (Bazeley & Jackson, 2013, p.2). The advantages of CAQDAS is not just managing large quantities of qualitative data (Noaks & Wincup, 2004, p.132), but also that it enables researchers to employ more codes and code data more quickly (Marshall, 2002, p.58). Nvivo software was used primarily for the practical considerations that both the software license and training courses in the package were available from the university. Nvivo was useful for the research design as it allowed more effective data management, for both text and audio files to be uploaded for coding, as well as to run reports and queries which assisted in data analysis.

A three stage process was followed to code and analyse the data. While the study was not designed to follow a grounded theory methodology, the process of coding

and analysis did draw from this tradition. The first stage of open coding used the *descriptive coding* method, assigning subject-based identifiers as free nodes within Nvivo resulting in a categorised summary of the data for subsequent coding and analysis (Saldaña, 2013, pp.88-89). During this process, topics from the interview data relevant to the research questions were identified and coded as well as, for the case study, useful contextual data with respect to the key features of FACT's operating model. Aiming for total theoretical saturation in which no further meaning could be extracted from the transcripts would have been a perpetual process if taken to its logical extreme (Marshall, 2002, p.61), so a manageable and pragmatic approach was taken. A comprehensive line-by-line approach was taken to coding, rather than employing a constant comparative approach. However, it was recognised as progress was being made that additional topics and codes were being identified in later interviews that had not been coded in the same way in earlier transcripts; it was considered prudent to re-examine the earlier transcripts where saturation had not occurred (Glaser, 1965, p.442; Glaser & Strauss, 1967, p.112). Accordingly, notes were made of key topics and codes used in coding later transcripts that had not been used in the earliest transcripts and these early transcripts were recoded. This re-coding was performed in detail for the first eight transcripts, but during the last few of these it was found that fewer coding changes were being made. Each of the transcripts was reviewed a further time to ensure that key topics had not been overlooked. On completion of the first phase of coding additional work was undertaken to tidy the codes, combining a small number where duplicates based on different synonyms of the same code had been created.

The second phase followed the tradition of *axial coding*, in which the data and codes were arranged and reassembled into thematic categories, to assist in identifying and developing the linked themes and meanings within the data. Bazeley (2009, p.7) observes the danger of named themes simply being meta-categories or classifications of codes, and states that emergent themes often closely resemble those already discussed within the literature (Ibid., p.9). At this stage, it was becoming clear that some themes did indeed follow issues discussed in the literature, which is to be expected, but also that other issues emerged that were not covered therein. Furthermore, repetition of some same topics across different transcripts and across interviews conducted in both phases of the research also provided validity for the findings by suggesting that the respective codes were reliable (Bereska, 2003, p.70).

A final stage involved analysis of the coded data into meaningful thematic categories, loosely following the concept of *theoretical coding* to create overarching codes into which the topics logically fall, resulting in a few core categories that systematically link the data (Saldaña, 2013, pp.223-224). To conduct this, all coded data were printed, analysed and mapped out on word processing and spreadsheet documents to determine the links and relationships between them and identify the central categories to which they ultimately related.

For the documents and field notes collected during the case study phase, a relatively simple approach was taken to content analysis. As these were collected primarily to provide macro-level context in relation to the case study – for understanding FACT as an organisation and additional supporting evidence of processes discussed during interviews – detailed line-by-line coding was not undertaken. Each document was examined closely and memos made as to how they related to topics from the interview data. By way of example, where copies of memoranda of understanding were obtained, these were analysed in terms of overall content and structure to add deeper meaning to the role described in the interview data that these tools played in facilitating information sharing.

Summary

The study employed a multi-method qualitative research design based on two discrete phases of data collection: a case study of a single organisation that relied strongly on effective information and intelligence sharing as a core process to combat intellectual property crime; and a series of stand-alone qualitative interviews conducted with representatives of other organisations that rely on information sharing as a means of combating economic crime, or other subject matter experts. This provided a substantial body of data which was coded and analysed in three stages, following a strategy incorporating elements of grounded theory.

The design can be evaluated as having provided an effective strategy for the collection of an extensive and rich body of data suitable for addressing the research questions. The greatest weakness of the strategy was that it was perhaps over-ambitious for the purposes and constraints of a doctoral research project, resulting in an extensive body of data being gathered which led to challenges in respect of transcribing, coding and analysis. Employment of either of the two phases alone may have resulted in the collection of a more readily manageable body of data that would arguably have been sufficient to answer the research questions. However,

completing both phases has undoubtedly provided a richer body of data to analyse, has helped validate the findings through triangulation of data and, most importantly, has enriched the findings and depth of the study.

The strategy has also been effective in terms of adding to knowledge in the subject area as it is the first time, to the researcher's knowledge, that a UK-based non-law enforcement organisation dedicated to combating crime, and the first in the intellectual property arena, has been the subject of a case study examining the way in which it shares information and intelligence with others.

The next chapters set out the key findings from the research, commencing with a review of findings relating to the barriers and challenges to economic crime information sharing and the legislative framework and problems that collaborating organisations must navigate.

Chapter Four

Findings: The Legal Framework and Inhibitors to Collaboration

Introduction

In this, the first of four chapters setting out the research findings, the focus is on outcomes relating to the contemporary challenges and barriers to information sharing. This has been structured in three parts. The first sets out participants' views on how UK organisations are performing in terms of information and intelligence sharing. The second part summarises key issues relating to the legislative framework around sharing discussed during the interviews, with special focus on data protection law. Finally, the other key challenges that were reported by participants as impeding effective collaboration are identified.

Performance of UK Organisations in Information Sharing

As a prelude to the second phase interviews, the interviewees were asked for their general views on how well, or poorly, organisations in the UK performed at information sharing, and if they could cite any examples of particularly good or bad practice. Although this was asked in order to solicit broad responses only, and the responses were not probed in detail, it provided some interesting results. Views varied widely, with some interviewees content that organisations were performing reasonably well overall while others relayed a more pessimistic assessment. Some went into more detail than others, and some restricted and clarified their responses with respect to particular sectors or industries. This data provides useful contextual information about how those involved in combating economic crime and sharing intelligence across a variety of sectors and industries perceive the current state of collaboration in the UK.

Some respondents were downbeat in their judgement of how organisations as a whole were collaborating:

> RI/07: "I think it should be a lot more fluid than it actually is, and I do find it a struggle reaching out to different organisations and trying to progress cases where there is a need to perhaps link in with other organisations."

RI/05: “Abysmally. Abysmally. I attended a conference, I spoke at a conference about a month ago at Hill Dickinson in London where it was it was entitled ‘Profile of a Fraudster’. And what Hill Dickinson were keen to do was to try and break down some of the barriers. […] And there were three people from the insurance industry sat on the panel […]. And the interesting thing that came out from that was when challenged by the chairman as to what they thought the initiative was the insurers said ‘to be honest, we don’t even co-operate with each other because if I reject a claimant or a policy holder and he goes to one of my competitors, I get a double win. I avoid the fraud risk but what I also do is I cause my competitor who’s less well-resourced or less intelligent than I am to take that risk and potentially therefore reduce their effectiveness or profitability in the space and therefore give me a competitive advantage’.”

Some of the less optimistic views were particularly focussed with respect to sharing within the public sector, or between public and private sectors:

RI/03: “I think it varies tremendously, I think there is a tremendous amount of inconsistency in terms of how it’s done. I think there is a massive disparity between public and private sector.”

RI/21: “A large number of the partners we work with are very comfortable sharing information with us. Others, you’ll probably recall yourself, the Revenue – HMRC – are somewhat unusual in that their initial stance is ‘you give us everything, we give you nothing’.”

RI/11: “And if you think information sharing between private and public sector is bad, then look at public to public, or police to police. Or police to law enforcement. It’s horrendous.”

However, not all responses were negative. Other parties took either a more positive view, or at least saw that there were signs that things were improving, perceiving a greater willingness to collaborate. This applied not only to private sector organisations, but also within the public sector.

RI/19A: “Looking at our industry [insurance] we’ve been notoriously bad for sharing intelligence and information. We’re getting better. Different sectors

are better than others, so motor is way far [sic] advanced in sharing intelligence than, say, casualty and property. […] But we're now seeing the frauds change, move into other areas such as casualty in terms of organised nature, and you immediately see how far behind those areas are in sharing intelligence because they're not used to doing it. So, you know, it used to be awful, it's made improvements, still much more room for improvement would be my view."

RI/04: "There are aspects of the public sector which, due to prior legislation, certain bodies within the public sector have been somewhat reticent to share information. However, I think there is I think a change in perceptions about fraud data sharing, fraud intelligence sharing. I think the last year, couple of years or so, have been a lot more participation in groups like the ACPO as-was working groups under the Economic Crime Portfolio. I think within those sorts of groups there's been much more willingness to share. We run working groups here which now people from the public sector are attending and sharing their fraud MOs verbally as well. We are establishing more connections within the public sector for the purposes of sharing things like MOs, intelligence, that sort of thing. So I think the situation is improving."

Two interviewees expressed very positive views about the current state of collaboration within the UK, although it was also evident that, for one of these, the optimistic opinion was relative to the challenges of sharing information in other jurisdictions.

RI/22: "So within the UK I think we do incredibly well, as it happens. I think the National Intelligence Model provides a good backbone for the exchanging of intelligence between agencies."

RI/14: "I think I'm quite qualified to say this, having worked in the UK all of my adult life and now looking after, for the last 18 months 2 years, looking after Europe, data privacy in Europe, I thought data privacy was prohibitive in the UK. Believe me, it's an absolute holiday in the UK. Europe is an absolute nightmare, and France in particular are so bureaucratic it's absolutely crazy, so I think – to qualify that – I think the data sharing is not an issue in the UK, providing you use data protection or whatever other legislation is available to you."

It is clear from the responses that there are a wide variety of opinions on the current environment for inter-organisational collaboration and sharing amongst practitioners. While the overriding theme was that the situation was not particularly healthy, participants from both public and private sector organisations indicated that there was a greater willingness and openness to collaboration being seen and that there is a positive direction of travel despite the problems that remain.

The UK's Legislative Framework for Information Sharing

A major topic of discussion within the interviews was that of the legislative framework within the UK with respect to information sharing including, most extensively, the law on data protection. That this was a significant focal point was no surprise. The Law Commission's review of information sharing (2014, p.3) concluded that there was a lack of legislative clarity, conflicting guidance and consequential problems in the practice of information sharing. Participants' views on the legislative framework covered a range of topics, covering the law as both an enabler of, and a challenge to, effective collaboration between organisations and sectors for combating crime.

Data Protection Act

The DPA is perhaps the most significant piece of legislation with respect to information sharing. Whilst it remains a contentious instrument that present numerous challenges in respect of collaboration, many of the interviewees expressed views that the legislation in itself was not a barrier to sharing. Thirteen participants from the second phase interviews, plus the most senior FACT officers, recognised that, properly applied, the Act could facilitate the legal exchange of anti-crime information. Three more participants discussed using the legislation in practice. Whilst it should be taken into account that participants were proactive proponents for sharing information, this does suggest broad consensus amongst practitioners that the provisions of the Act should enable collaboration.

> CS/24: "I carry around a copy of the Codes of Practice of the Data Protection Act, and I keep showing... This key issue is that people do not understand that just because you're a government agency, a law enforcement agency, a private agency, it doesn't matter. The Data Protection Act talks about, the word they use is 'organisation'. That's the word they use. So any organisation, no matter who you are, government, local authority, police,

private, you can share information. You must have the checks and balances in place, but you can share that information."

RI/03: "I actually think [DPA section] 29(3) works pretty effectively, to be perfectly honest with you. I think if you understand the legislation, if you engage with the regulators, if you operate a sound business model with good governance and you have proper controls around it, then I think 29(3) as it stands already provides a good framework."

RI/06: "And as long as the information is shared in a compliant manner with those proper checks and balances and a mechanism to do it, then absolutely. The DPA is not there to prevent you exchanging data, it's there to get you to exchange data in a compliant manner."

However, for all of the practitioners' recognition that the DPA may help facilitate data sharing if it is used correctly, it was also widely cited as being an impediment to collaboration in practice. The Fraud Review (Fraud Review Team, 2006b, p.100) noted that the Act was commonly misunderstood, and evidence from a large number of participants suggested that this was still the case.

CS/24: "From a legal perspective it's, the misunderstanding or the misinterpretation of the Data Protection Act is the biggest problem. It is, for intelligence sharing."

RI/12: "Some of the agencies don't necessarily understand data protection, and will say 'well I can't share that'. Well actually, yes you can because s.29(3) says you can for the purpose of investigating and detecting crime. So they don't have an understanding but we can persuade that."

Simple lack of understanding or misinterpretation is not the only challenge, however. One of the interviewees commented on a government department adding additional criteria not contained within the Act itself:

RI/01: "If you put forward a 29(3) notice stating exactly what you want the information for, the DWP some years ago went down the route of saying 'I can't help you it's not a serious crime'. Well, where does it say 'serious' in the Data Protection Act? It doesn't, so where did that come from?"

There were sometimes conflicting views from private sector participants on how well the Act was understood by law enforcement agencies:

> RI/19A: “I think it is a really good opportunity to share intelligence. You know, police get it completely, we’ve no problems with sharing with them because everyone understands it from an insurer perspective.”

> RI/14: “I think probably law enforcement don’t understand. Having been for 30 years in law enforcement I don’t think law enforcement understand data protection. I think frequently you will get someone bowling up with a s.28 [sic] DPA request. Well, what they don’t understand it’s not mandatory. I’m the data owner, and I can refuse.”

Frustrations relating to the DPA were expressed by most participants in the second phase of the research, and by some in the case study, and several criticised the ICO for failing to provide clarity on the issue.

> RI/18: “The Data Protection Act and the understanding of that is a big problem. And the reluctance of the Information Commissioner’s Office to come out and make a clear statement again is problematic.”

Another frequently cited complaint was that the DPA was used by many people and organisations as an excuse to hide behind, rather than to share data, regardless of the real reason for their unwillingness or inability to collaborate.

> RI/07: “My experience shows me that a lot of companies use the Data Protection Act to hide behind rather than using it as an opportunity to share information and intelligence. So I find it quite a frustrating notion, I guess.”

> RI/21: “You may well, and we do, find individuals who choose to interpret legislation or who choose to interpret management guidance as a reason not to do something. You know, we frequently hear that the ‘oh we can’t tell you that because the Data Protection Act doesn’t allow us.’ And of course we go back then and say ‘if you look at the reasons to share this information, you’ll find the prevention and detection of crime is a specific exemption.’ But you’ve

already backed someone into a corner that they were comfortable in their position and sometimes you will not move them from that position."

This issue was also recognised and discussed by an interviewee who operated within the regulatory environment:

RI/08: "Plenty of people hide behind the skirts of data protection law as well because they just don't want to do something, and it's easier to say 'oh the Data Protection Act doesn't allow me to do it', rather than say 'I don't want to do it', because that sometimes causes offence."

The other commonly discussed issue with respect to the DPA was that organisations are afraid of making mistakes with respect to sharing personal data and of the potential consequences of doing so.

RI/06: "There's a reluctance, in my opinion from a lack of understanding of the Data Protection Act to actually exchange information. Everybody is terrified of getting on the wrong end of the Information Commissioner, of exchanging information and being criticised for it, if not prosecuted for it."

CS/17: "I think people are worried about it. People are frightened of it. Because it's a stick to beat people with."

RI/13: "The second issue is that culturally, is there a cultural imbalance when it comes to information sharing? So if you look at, you can cast your eye over the Information Commissioner's Office and look at people who've been fined and organisations that have been fined £10,000s, sometimes £100,000s, for loss of information. So what I'm saying is quite rightly there's an oversight on how information is handled. But can you tell me many examples where people have been fined £100,000s or threatened with imprisonment because they've failed to share information?"

RI/13 was not the only person to comment on this perceived imbalance:

RI/01: "…if you share data erroneously, the individual is held to account by the Information Commissioner's Office, and if that goes wrong, or people lose data or a laptop gets misplaced, it's all over the papers, and people or

organisations get significant fines and that's all over the papers when something goes wrong. But it's never in the papers when something goes right. And an awful lot of data does get exchanged properly."

The DPA, therefore, is a significant issue in the UK's information sharing environment and was a major topic of conversation within many interviews, especially in the second phase of the research. While most practitioners took the view that it provides adequately for the sharing of information under the right circumstances and with adequate controls in place, the real problem was with misinterpretation and misapplication of it. For this reason, some considered that reform would be justified.

The Wider Legislative Framework

While the DPA is a significant piece of legislation relating to information sharing in the UK, especially with respect to private sector organisations, it is just one part of a wider framework of legislation. The interviews covered different aspects of the legislative framework in varying degrees of detail according to interviewees' perspectives. It is clear from the data that the overall legislative environment is perceived to be complex, convoluted and opaque; a situation which emphasises the challenge for those seeking to engage in inter-organisational data sharing. This section will summarise interviewees' views with respect to one specific piece of legislation – the creation of SAFOs under s.68 of the SCA – and then review the data relating to two further topics: legislation and legal gateways governing government departments and agencies; and the effectiveness of the legislative framework as a whole.

SAFOs

The establishment of SAFOs under the provisions of the SCA was discussed in Chapter One. Several interviewees represented organisations that had obtained SAFO status meaning that, for the purposes of the legislation, they were designated as organisations with whom public sector bodies could collaborate for anti-fraud purposes and which had appropriate systems and controls in place. This provision was discussed with these participants to obtain their views on how helpful this status was. The responses were generally positive, to an extent; most suggested that it was useful to have the status, but that it hadn't necessarily opened a channel to extensive collaboration with the public sector. Three participants (RI/03, RI/04, RI/06) suggested that SAFO status had helped them to add public bodies as member organisations, and that the designation provided reassurance for those organisations. However, two interviewees (RI/06, RI/17B) commented that when they sought to

engage with public sector organisations, these still weren't aware of the legislation or what SAFO status represented, and that there was still reluctance to engage when they were aware of the provision. RI/03 also stated that his organisation would find it difficult to quantify the value of SAFO status in terms of data that was actually shared due to the provision. RI/02, who is a policy lead on data sharing for a government department, stated that while the legislation had the potential to make a difference, it did not work effectively in practice. This data supports the findings of reviews conducted into the efficacy of the channel (NFA, 2010a, pp.16-17; ICO, 2015, p.15).

Departmental Legislation and Information Sharing Gateways

Broad gateways such as SAFOs, designed to enable cross-sector sharing, aside, the prospect of collaboration between sectors was recognised to be a complex issue. Several interviewees discussed the difficulty of engagement and collaboration between public and private sector organisations due to restrictions on some government agencies and departments set out within their primary governing legislation, or *vires*. RI/01, RI/03 and RI/12 discussed specific statutory restrictions within which organisations such as HMRC and the DWP had to abide, with RI/01 pointing out that, because of these, they could not fall back on the anti-crime disclosure exemptions set out in the DPA. RI/02 observed that, consequentially, we have reached a situation in which some bodies are bound by defined statutory limits and for which positive powers to share information must be created, while others are bound by common law and can collaborate unless there are specific restrictions against doing so. This situation is complicated further given the numbers of legislative instruments that may apply and that it is often not clear which take precedence when these overlap or conflict (Law Commission, 2014, p.13).

Another problem discussed by participants was that of the number and specificity of gateways established by legislation. Given the Law Commission's (2014, p.26) finding that there were too many specific statutory gateways enshrined in legislation providing data sharing powers for defined circumstances, it is no surprise that this was a matter that concerned participants, who were disparaging about the complexity of the resulting information sharing landscape.

Several participants, including RI/01, RI/02, RI/13, RI/20 and RI/22, discussed the multiple legislative gateways and the over-complexity that arose from these. The specificity of these gateways was also cited as a problem. RI/02 suggested that not

only did this add a significant amount of time to the already lengthy process of creating data sharing agreements through negotiation between parties as to which gateway was appropriate to use, but that many gateways were so specific it prevented flexibility in how the data could be used for combating fraud:

> RI/02: "So you'll end up with situation like DWP and local authorities when it comes to housing benefit data where they're sharing this housing benefit data and it's for the local authorities to only pursue housing benefit fraud. That data is incredibly rich data and very useful for local authorities should they wish to pursue tenancy fraud. However, the agreement with the DWP and with the gateway that was put in place did not mention tenancy fraud because they didn't think about it at the time."

Several interviewees, most explicitly RI/02, RI/13 and RI/20, called for a process of simplification and codification of these provisions. RI/01 contrasted the legislative trend with respect to the creation of myriad gateways to that of the simplification of anti-fraud legislation, noting that the Fraud Act had created a small number of general fraud offences, whereas the government was creating a large number of very specific gateways to deal with different types and circumstances of fraud.

Adequacy of Legislative Provision

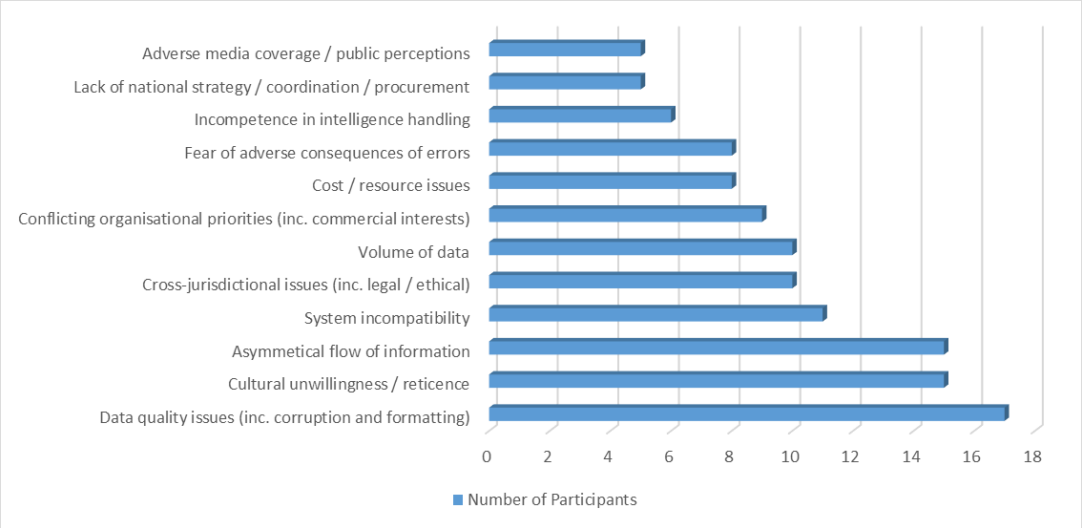
Given the complexity of the legislative provisions in the UK, it is perhaps unsurprising that participants' views on whether or not current legislation was fit for purpose were varied, with a fairly even split between those that took the overall position that there was adequate provision within current legislation to enable effective information sharing between organisations (including RI/03, RI/04, RI/06, RI/11, RI/14, RI/20), and those that pressed the need for legislative change (including CS/17, RI/01, RI/02, RI/12, RI/13, RI/15, RI/18). Amongst those who considered that current legislation provided sufficient channels for legal exchange, many still suggested that simplification, elucidation and guidance would be beneficial. Many of the calls for change concerned the same issues, mostly calling for the creation of clear, general gateways and the reduction in complexity and specificity of these to reduce the legislative tension between adequacy of provision and the reduction of uncertainty.

> CS/17: "I think the demystification of what the rules are is so important. Because if you don't understand what you can and can't disseminate, you're never going to be able to effectively share intelligence with anyone, are you?"

Additional Barriers and Challenges to Information Sharing

While legislative matters were a significant topic of the data collection interviews, these were not the only impediments to information and intelligence sharing discussed. Due to the wide variety of organisations whose representatives took part in the study, a range of challenges were discussed, many of which were organisation- or sector-specific. However, a number of issues cited as challenges to effective collaboration were discussed the interviewees, and those most commonly referenced are summarised in Figure 4.1 below.

Figure 4.1: Barriers and challenges discussed during research interviews



The most commonly discussed issues across the sample concerned cultural challenges to sharing, such as information flowing in only one direction between information sharing partners and the underlying unwillingness of some people and organisations to collaborate, and more technical problems relating to the transfer of data. While these were the main topics directly discussed in terms of barriers to information sharing by the participants, other issues, such as the necessity of trust and adherence to shared standards were also discussed during the interviews, allowing the inference to be drawn that the converse of some of these positive factors would also impede collaboration.

Summary

In this chapter, the views of participants on the current state of information and intelligence sharing in the UK, including on the legislative environment, have been set out. The findings have been mixed, with some practitioners more positive than others

on how well organisations in the UK perform in respect of sharing, although there does appear to be more willingness to engage experienced in recent years. The legislative framework within which sharing must take place, however, is seen as over-complex and difficult to navigate; this is invariably seen as problematic both by those who consider that current legislation provides adequately to facilitate sharing and those who suggest that legislative reform is necessary. In addition to the legislative issues, a range of additional challenges and barriers have been identified as continuing to inhibit information sharing between organisations.

The following three chapters will set out the findings of the research in respect of the structures, processes and strategies of organisations to collaborate effectively despite the challenges faced. The next chapter will provide an overview of FACT, which was the subject of the case study phase of data collection, examining its structure, functions and approach to partnership working.

Chapter Five

Findings: Matter of FACT – Case Study Overview

Introduction

This chapter will examine FACT as an organisation based on the findings of the case study phase of research. FACT will be described with respect to its role, structure and functions, how it operates and the fundamental approach taken to intelligence processing and sharing with its partner organisations.

Case Study: The Federation Against Copyright Theft

The case study data collection was conducted by spending two weeks at FACT's office in Twickenham. The data collection involved conducting interviews with senior officers and staff members across each of its core and support functions, collection and review of documents relating to strategies, policies and operations, and conducting observations. The outline of FACT set out below is drawn from review and analysis of data collected during this fieldwork.

Overview – History, Mission and Operational Focus

FACT was formed in England in 1982 and incorporated at Companies House in October of that year. The original name upon incorporation was Webcast Ltd, although the name was changed to the Federation Against Copyright Theft in November 1982, and a revised incorporation certificate issued by the Registrar of Companies in January 1983. It was registered as a non-profit making company limited by guarantee, without share capital. In the documents issued to Companies House notifying it of the change of name, the organisation also reported details of its starting membership on whose behalf it was to work. This comprised nine organisations, including six major companies in the film entertainment industry and three trade associations: the Motion Picture Export Association of America (now the Motion Picture Association [MPA]), the Society of Film Distributors and the British Videogram Association (FACT, 1982, p.2).

The Director General (CS/18) described FACT as a trade organisation, which remains non-profit making, representing the interests of its members in terms of protection of copyright material and pursuing enforcement action against those that unlawfully infringe their content. FACT originally came into being due to the widespread copying

of the film E.T. onto video cassettes (CS/18), and thus was created to tackle the issue of film piracy.

FACT's primary operational activities involve work in three key areas of copyright infringement:

- prevention and detection of illegal recording at source (e.g. in cinemas)
- combating online piracy and the unlawful and unauthorised distribution of copyright material online, including digital streaming and file sharing
- detection and disruption of piracy in hard media, such as pirated DVDs and decoders, often involving organised criminal groups (FACT, "About FACT", 2015a).

Figure 5.1 provides some examples of FACT's enforcement activities.

Figure 5.1: Example FACT cases

FACT Case: Counterfeit DVDs

In November 2016, the manager of a Post Office branch in Southwark was jailed for 25 months for selling over 7,000 counterfeit DVDs. He imported the goods from China, repackaged them from his home, sold them online and posted them from his Post Office branch. FACT discovered the crime, which was investigated by Trading Standards officers and prosecuted by Southwark Council, demonstrating the value of multi-agency collaboration. He was jailed for offences under the Fraud Act 2006 and the Trade Marks Act 1994.

Source: FACT ("Post Office manager", 2016e)

FACT Case: Illegal Online Film Releases

In December 2015, in the first ever criminal prosecution for an online release group, five men were jailed for a total of 17 years for illegally releasing films online. Over several years, they made over 2,500 films available online, which were downloaded millions of times. Each of the convicted men accepted liability for a criminal loss of over £1 million, with the collective loss in excess of £5 million. The convictions were secured following an investigation led by FACT, working with several partner agencies including the police and the Intellectual Property Office.

Source: FACT ("Online movie release", 2015b)

FACT Case: Illegal Public Display of Sports Broadcasting

In November 2016, FACT successfully prosecuted two pub owners in Leeds for showing live sports events in their pubs without having the correct licences and agreements with Sky Sports to do so. Both received fines, which totalled more than £8,500.

These convictions brought the total number of convictions since the start of the 2016/17 football season to 22 by mid-November, with total fines issued by the courts exceeding £90,000.

Source: FACT ("Two Leeds pubs", 2016f)

In respect of these activities, FACT operates a strategy covering various pursuits, including raising awareness, conducting investigations – often in conjunction with other organisations – and pursuing litigation and sanctions. For the latter, it will work

closely with law enforcement partners to seek to advance cases to public prosecution, although in some circumstances it does pursue private prosecutions on behalf of its members. It has a successful enforcement strategy, securing 553 criminal convictions in 2009 (FACT, 2013a, p.4), although it actively pursues other interventions as well, working to prevent, disrupt and dismantle criminal operations (FACT, n.d., p.4). FACT seeks to get involved in political and media debate about intellectual property and the availability of entertainment media to counter the arguments of those who advocate that all such material should be freely available (CS/18). It also has an interest in political lobbying, primarily by supporting other organisations that actively lobby in this area.

FACT also operates a certification scheme to organisations operating within the visual entertainment industry. Through this scheme, organisations operating at any stage of the supply chain, from filming studios to the point of distribution (e.g. cinemas, TV studios and retailers), as well as distribution and logistics companies, can apply for FACT certification. Certification is given following an inspection of premises, security controls and policies (such as staff non-disclosure agreements) and represents a benchmark of reliability confirming that the accredited company has appropriate controls in place with respect to handling intellectual property. Continuing certification is subject to annual inspections and fees, and this provides both a service to the industry as well as income to FACT. It can also be a source of intelligence (CS/10) for FACT. During interview, the Certification Manager (CS/10) suggested that approximately 140 companies held the certification, although by late 2016 the published register indicated that 109 companies were accredited through the scheme (FACT, "FACT Certified Directory", 2016b).

In 2016, after the fieldwork had been completed, FACT extended its services beyond the film and television industry to encompass wider content and brand protection offerings (FACT, "FACT launches services", 2016c). However, these activities fall outside of the scope of this thesis.

Membership and Funding

As FACT is a membership organisation, a primary source of income is from its members, which pay annual fees according to a multi-tier subscription structure based on their turnover. At the time of data collection, FACT had seventeen members and was in discussions with other prospective parties (CS/18). Membership numbers do fluctuate; at the end of 2014, FACT had twenty-four members (FACT, 2014, p.2),

while in October 2016 it had twenty-two (FACT, “Members”, 2016d). While all members pay towards FACT’s operating costs, the majority of funding (55%) at the time of data collection was provided by the MPA (CS/18).

According to its financial statements to 31 December 2014, FACT’s turnover was £3.04 million, of which £2.87 million was derived from membership subscriptions, with additional operating income of £0.8 million (FACT, 2014, pp.8-11). Income is also derived from the certification scheme and additional funding is received from Sky and BT Sports (in excess of their membership fees) for the prosecution of publicans and others for illegally showing live sports. Occasionally, additional income is received from other sources, such as a £10,000 payment from the Cinema Exhibitors Association to allow FACT to purchase new software to capture and manage intelligence from social networking and other online resources (CS/18).

As FACT is a not-for-profit organisation, it aims to balance the books without deficit or surplus. When there is a surplus, this is reinvested or transferred to the legal fund used to pursue prosecutions on behalf of members (CS/18).

Governance and Management

FACT has a board of directors comprised of member representatives. Not all members are entitled to representation on the board; this is restricted to those that pay subscriptions in the top four membership tiers (FACT, 2016a, pp.9-10). The board appoints a Director General and other directors who need not be appointed from the membership. At the time of conducting the research, the Director General was an executive officer of FACT and not an employee of any of its members. FACT’s constitution states that there is no requirement to appoint a company secretary (FACT, 2016a, p.11), unless so required by legislation, although in practice it does make an appointment to this role.

Oversight is provided by way of board meetings, to which the Director General reports, and additional General Meetings are held which are open to the wider membership to include those not represented on the board. Members are assigned different voting rights according to their membership tier (FACT, 2016a, pp.7-10). FACT is also constitutionally required to hold an Annual General Meeting.

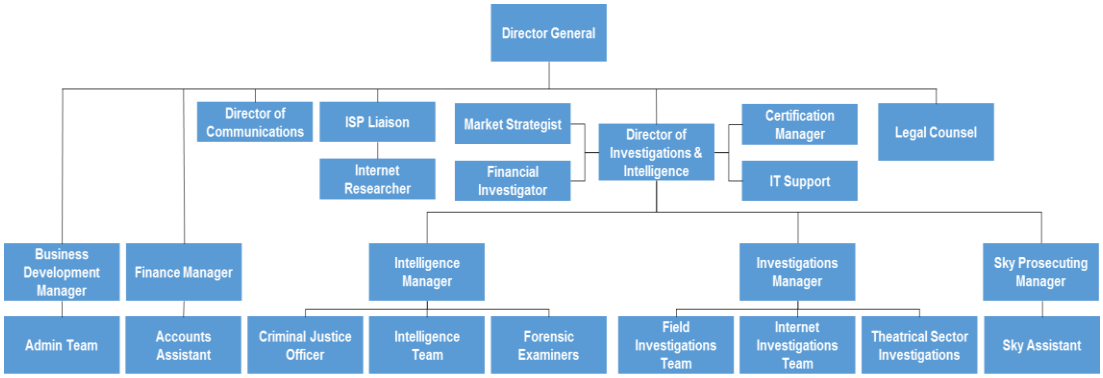
In terms of operational management, the Director General has a deputy, the Director of Investigations and Intelligence, beneath whom sit middle managers that lead the

individual business units. The other key officer is the General Counsel, who is a FACT employee. The HR function is the responsibility of the Business Development Manager, who maintains control over staff policies and procedures. Recruitment is generally conducted through agencies, with two trusted agencies relied upon for most appointments (CS/10).

Organisational Structure

FACT has a relatively flat operational structure. Figure 5.2 provides a high level overview of the structure down to the key operational and support functions, adapted from a more detailed organisation chart provided by FACT (2013b, p.2).

Figure 5.2: FACT organisation structure (high level)



The core operational units are the Field Investigations, Internet Investigations and Intelligence teams, supported by the Forensic Examinations (IT forensics) team and additional operational and back office functions. At the time of data collection, FACT employed approximately 42 people, although a number of additional positions were vacant. The headcount has since fallen due to internal restructuring and a reduction in funding from the MPA (FACT, 2014, p.3), so Figure 5.2 may no longer accurately represent the current structure.

The Nature of the Threat

The intellectual property theft that FACT seeks to combat is both complex and damaging. Traditionally, film piracy involved the manufacture and sale of counterfeit DVDs and video cassettes. DVD piracy was still an issue at the time of fieldwork, but the methods of distribution of these goods was shifting away from markets and car boot sales to online sale via direct sale websites and social media platforms (FACT, 2012b, p.5).

Most film and TV content theft now takes place online (FACT, 2013c, pp.3-4), with criminal groups using file sharing and live streaming sites to host and distribute content online. Illicit streaming of live sports is also predominantly online, although there are additional angles of hardware infringement allowing access to subscription content in the home without payment, and of pubs and other venues screening live sports without holding the relevant licences.

There are three main types of motivation behind this type of IP crime. For 'release groups', which recruit 'cammers' and 'cappers' to record video and audio respectively at cinemas for subsequent online release, the motivation is primarily for the kudos of being the first to make new releases available (CS/18). 90% of online film content originates from recordings made in cinemas (FACT, 2012a, p.1). Criminals running file hosting, downloading or streaming sites are largely separate to release groups and are motivated by financial gain (FACT, 2013c, p.20), achieved by selling access to illicit content and selling online advertising space. The sale of hard goods is still dominated by organised criminals, primarily Chinese gangs in England, and local crime groups in Scotland and Northern Ireland. Profits are used to fund other criminal enterprises, including human and drug trafficking (CS/18).

Losses to the UK film and television industry are conservatively estimated to be £0.5 billion per year, and criminal profits approximately £200 million per year (CS/18).

Organisational Ethos

Because of the changing landscape in how people perceive, access and consume film, television and sports entertainment media, FACT had to undergo a fundamental change in its structure and approach during the tenure of the current Director General. When he arrived, FACT was still geared towards disrupting the distribution and sale of pirated video cassettes and DVDs. In the intervening years, it was re-orientated towards internet-based IP crime through peer-to-peer file sharing and digital streaming, as well as crime relating to satellite decoders and illegal public performance. As technologies advance quickly, FACT's leadership recognises the need to adapt to changing threats.

As such, it has adopted an intelligence-led ethos, works broadly in line with the NIM and has invested heavily in intelligence software (CS/18). It works closely with numerous bodies in the law enforcement, government and intellectual property

arenas (CS/23, CS/24). The intelligence function, and the accuracy and quality of its intelligence database, is cited as being at the heart of FACT's structure:

> CS/18 "…every decision we make is based on what we know because of the intelligence that we've developed. So the intelligence unit is the hub of the organisation. Everything else is subservient to that. […] All the other units: the internet investigations team, the field investigators, the forensic examiners, even the individual people – the cinema investigators; everything that they do has to go into the intelligence team. […] Using intelligence to build a case and make informed decisions on what resources you're going to put into it and continue to examine your goals and objectives and see if they're still achievable. Absolutely imperative. It works, and I can prove it works, and it's the only way forward."

An important feature of FACT's ethos towards intelligence and collaboration is the attitude taken to information asymmetry; a key problem in many information sharing relationships (Zheng et al, 2008, p.95). FACT accepts that much intelligence sharing will flow in one direction, but this does not reduce its commitment to collaboration. Neither does it influence the perception of the value of information sharing to FACT, as attested by the Intelligence Manager and Director General:

> CS/24: "I think that always happens. The reality is we've got more to gain by giving it than keeping it. So my philosophy is if we can, share it. Give it to them. […] So the important thing is if we can share it, share it."

> CS/18: "What we do know, and what we say when we're doing it, is we realise that as a public organisation the chances are that you're going to get a lot more information out of us than we're going to get out of you. But we accept that."

This approach may be simpler to rationalise for FACT than some other organisations as it has numerous active channels of incoming intelligence, and that many of its relationships are reciprocal (CS/24), but this is a notable feature of its approach to collaboration.

Alignment with the National Intelligence Model

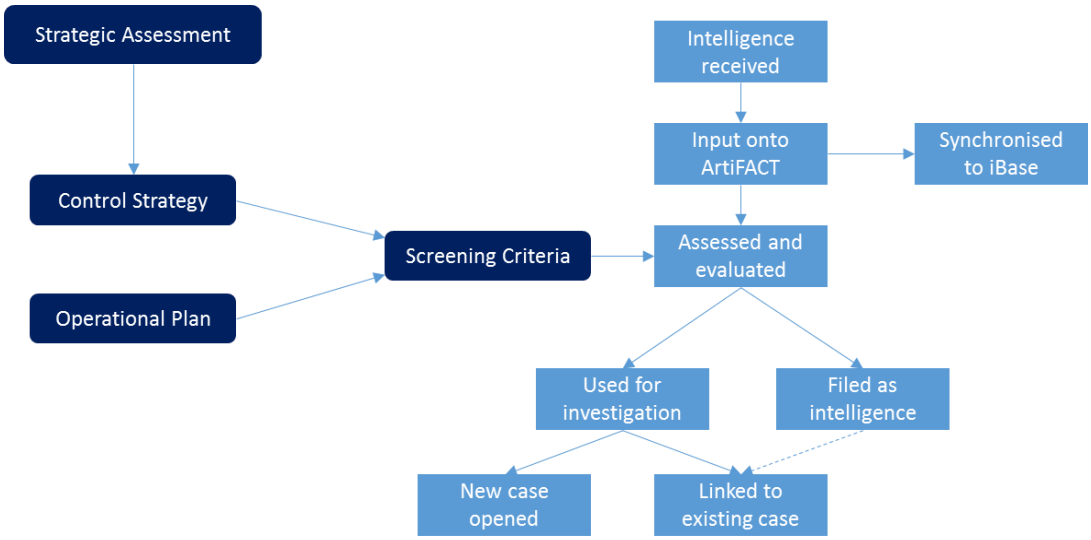
FACT has aligned many of its business processes with the NIM, this being considered essential as an intelligence-led organisation (CS/18). Its Intelligence Team works according to the NIM business model and adherence to this, and to the quality of the intelligence products produced, is integral to achieving its mission and effective collaboration with partners:

> CS/22: "…it's integral because all the police forces obviously abide by the NIM. When they know that we do as well, and we produce the same kind of products that they do it's obviously a lot easier for them to work with us. And they're seeing the same products that they would see from their own analysts and, more often than not, when they see our products they wish their analysts produced the same quality of products."

While FACT is not rigidly bound by the NIM (CS/18), it has aligned its business model, and several processes and outputs, to the NIM framework. This includes investment in the intelligence systems and processes used, the policies and procedures in place with respect to handling sources (including covert human intelligence sources [CHIS]), its evaluation processes, its development of intelligence and intelligence products (ACPO Centrex, 2005, p.15; ACPO Centrex, 2007, p.8), and debriefing at the end of investigations.

A Strategic Assessment is produced annually by the Intelligence team. This provides a comprehensive assessment of the threat environment, based on intelligence and research relating to threats and trends arising from new investigations, and takes account of emerging changes in that environment such as changing technologies and criminal techniques. This assessment is used to drive the control strategy, in line with the NIM (ACPO Centrex, 2007, p.12). The control strategy informs the intelligence screening criteria that FACT applies during assessment of incoming intelligence (CS/22) as summarised in Figure 5.3. The strategic assessment was considered by John and Maguire (2004a, p.25) to be potentially the most significant NIM intelligence product because of this influence on the organisation's control strategy. Additionally, FACT uses the Strategic Assessment as a tool to help inform partner agencies about the IP crime landscape in which FACT operates (CS/18).

Figure 5.3: Assessment of incoming intelligence at FACT



The NIM mandates a tasking and coordination process to drive operational decision making and allocation of resources (Police ICT, n.d., pp.2-4). While FACT does not run its meetings in precise alignment with the NIM model, it does conduct monthly Tasking and Coordination meetings at which all active cases are reviewed, and at which resourcing decisions are taken. One of these meetings was observed, by permission, during the data collection.

FACT's adoption of the 5x5x5 model of intelligence report (Appendix 18) for the evaluation of incoming intelligence and for dissemination of intelligence externally, is also in line with the NIM. John and Maguire (2007, p.206) observed that the core advantage of this model was to allow allocation of resources according to the quality of incoming intelligence. A new model, the 3x5x2 system (Appendix 19) was introduced in 2016 to overcome problems with the 5x5x5 (James, 2016, pp.86-87), incorporating clearer standards on how intelligence may be disseminated (College of Policing, "Intelligence report", 2015b). This was introduced after completion of the case study fieldwork.

Alignment with the NIM is central to FACT's strategy for effective collaboration, and to its own intelligence handling procedures.

Operational Structures and Functions

The following sections provide an overview of the main operational functions within FACT, with the greatest emphasis placed on the role of the Intelligence team and on how FACT collaborates with partners.

Intelligence Team

FACT's Intelligence team maintains responsibility for assessing, processing and developing intelligence received, providing analytical support for investigations and creating intelligence products for internal use, for sharing with partner organisations and for supporting litigation. The team, headed by the Intelligence Manager, is comprised of Intelligence Analysts, Intelligence Researchers and the Criminal Justice Supervisor, who also acts as Disclosure Officer.

The intelligence function uses the iBase intelligence management system [IMS] database on which FACT's intelligence records are stored. Intelligence is received from a variety of sources, including from law enforcement agencies and other partners, from members, from Crimestoppers and direct referrals from the public, as well as internally developed intelligence from investigation work (CS/22, CS/24). All intelligence received is input into the ArtiFACT case management system [CMS] (a modified version of the Cyclops CMS). This is performed by the person receiving the intelligence, who may be on any core or support team, and is input into ArtiFACT to a standard that enables ready conversion to a 5x5x5 intelligence form (CS/04). Once intelligence has been input into ArtiFACT, it is assessed by the Criminal Justice Supervisor who applies FACT's screening criteria. This informs the decision as to whether the intelligence leads to an investigation (or is linked to an existing investigation) or is just stored on the intelligence database for cross-referencing against future intelligence receipts (CS/04, CS/24). The Criminal Justice Supervisor is also responsible for creating cases and assigning analysts and investigators on the CMS (CS/22). All intelligence received is pulled into iBase for indexing within 24 hours after being input onto ArtiFACT (CS/17).

Intelligence received is sanitised by the Researchers as needed (CS/21) and linked to other relevant records. Intelligence evaluation is undertaken according to NIM standards and in line with the 5x5x5 system. The Researchers are tasked by the Analysts, or by investigators or senior managers, to develop intelligence by performing additional open source research upon it. They use resources such as electoral roll, land registry and credit reference checks and additional resources such as the National Anti-Fraud Network, and produce intelligence summaries of these (CS/21). Researchers also produce 5x5x5 intelligence reports for distribution to partner agencies, such as the police (CS/21, CS/24). All intelligence reports prepared for dissemination to partners are reviewed by the Criminal Justice Supervisor to check

that the appropriate evaluation codes have been applied (CS/04). Most intelligence disseminated to partners is issued on 5x5x5 intelligence forms as these are understood by the recipients, meaning that they are more likely to act on them:

> CS/17: "Our intelligence tends to be disseminated amongst, predominantly, law enforcement bodies or bodies that are associated with law enforcement by proxy, so IPO [Intellectual Property Office]. So they will understand a 5x5. So the great thing is we run by the National Intelligence Model, so we run by 5x5 reporting. The great thing that that allows us to do is everybody pretty much knows what a 5x5 is, to a certain extent. And if they don't, they're pretty easy to work out anyway. So we run to that National Intelligence Model standard, whereas a lot of corporate bodies that disseminate information don't."

Intelligence Analysts are responsible for providing analytical support to investigators and for creating intelligence products for internal and external use (CS/17, CS/22). A range of intelligence products are produced, including problem and subject profiles, composite 5x5x5 intelligence reports, timeline charts and visual association charts produced on i2 Analysts Notebook software, which provide a clear visual depiction of the relationships between entities and objects within investigations (such as people, companies, addresses, websites, telephone numbers, email addresses and bank accounts). The benefit of producing and disseminating intelligence in these formats – 5x5x5 intelligence reports and i2 charts – are not only that FACT's partners understand these, as noted above, but that the visual depictions especially are appreciated and understood by the police, courts and juries.

The Intelligence team places considerable value on the close relationships that it has with partner organisations, which are seen as vital to its business model. Significant emphasis is placed on FACT's reputation for producing high quality products, ensuring that partners can rely on the intelligence and evidence that FACT produces (CS/24).

> CS/24: "…our quality is very high, we set our standards very high. I do set a gold standard in what we do. But when we're not an enforcement agency you have to have the gold standard. They have to go 'oh, I don't have to do anything. I can take action, I can disseminate that further, it's all been done for me'."

To strengthen these relationships the Intelligence team routinely meets and engages with key partners. The Intelligence Manager attends Government Agency Intelligence Network [GAIN] meetings across the country, and regular meetings are held with the IP crime community group and the NFIB (CS/22). It has a close working relationship with the IPO (CS/24) to the extent that it shares a weekly report on all intelligence received, produced for FACT's internal use, with the IPO, subject to the relevant handling and dissemination codes (CS/21). FACT provides this in an Excel spreadsheet format to ensure that the IPO can import the data into its own systems, despite using a different format for its own purposes. The Intelligence Manager also provides training to some partner agencies, such as Crimestoppers, to ensure that their operatives understand the role and needs of FACT and therefore improve the quality of the intelligence that comes in (CS/22).

Field Investigations Team

The Field Investigations team is one of two investigative units falling under the Investigations Manager, and conducts investigations into cases of suspected intellectual property crime.

The field investigators are regionally based and focus on their own regions, although will assist investigations in other regions where necessary. The role involves a wide range of activities relating to the conduct of investigations into IP crime. The investigators tend to be ex-police personnel, and thus usually come into the job well trained in investigative skills (CS/11, CS/18). A large part of the role involves working closely with partner agencies, such as the police and Trading Standards officials. Their work involves putting together case materials, taking part in raids, assisting in interviews, advising on legislation relating to IP crime and providing statements (CS/01, CS/09). They also build and develop relationships and contacts through attending forums and GAIN meetings (CS/01). Investigators will be the usual point of contact for law enforcement partners throughout a case (CS/09), and work on case management after suspects have been arrested by police (CS/18).

They also regularly undertake operations during investigations conducted by FACT, such as test purchases and some surveillance activities (CS/11, CS/23). Careful control is maintained on these procedures, with authorisation processes mirroring the requirements of Regulation of Investigatory Powers Act 2000 [RIPA] legislation, despite RIPA not applying to private companies. All surveillance activity is subject to

assessment and approval by the Director of Investigations and Intelligence by way of a Directed Surveillance Authority (CS/23).

Historically, the focus for the field investigators was on crime relating to the manufacture and distribution of counterfeit hard goods, such as DVDs, although, along with the rest of the organisation, the onus is moving more towards online crime. One of the investigators, CS/09, suggested that only 10% of her time is now focussed on crime relating to hard goods. However, this is variable depending on region as there is more hard goods-related crime in major cities and this is a greater problem in deprived areas, such as Glasgow and parts of Northern Ireland (CS/11). Investigators in these areas will spend more of their time tackling those issues.

Internet Investigations Team

The Internet Investigations team also reports to the Investigations Manager. Its role is to conduct investigations, collect evidence and seek interventions against internet-based criminals infringing the copyright content of FACT members. This includes investigations into streaming sites, torrent sites, sites streaming live sports matches and cyber lockers, as well as sites selling counterfeit DVDs and other hard goods online (CS/14, CS/15, CS/20). The team is comprised of a number of investigators, a supervisor and an internet researcher.

Internet investigations are conducted to establish the underlying facts about websites of concern, and involve work to verify that sites make copyright content available without the necessary permissions and authority. The investigators gather evidence about the nature of the site, who runs it, where it is hosted, the amount of traffic on the site and evidence of monetisation of the content (CS/14, CS/15). The team also conducts scanning projects, using a semi-automated web crawler that crawls through torrent sites and identifies members' content, the results of which are verified and evidenced by the team (CS/14). These investigations are conducted with a view to seeking interventions, ranging from issuing takedown notices under the US Digital Millennium Copyright Act [DCMA], issuing Google takedown requests, knocking on site owners' doors to confront them directly, through to criminal prosecution (CS/15).

The team also conducts covert activity, with one of the team members having developed a number of aliases over the course of several years which have gained credence amongst the IP criminal community. These are used to gather intelligence through interacting with this community. This activity does require a limited level of

participation by providing copyrighted content online in order to maintain criminals' trust in the identities used. FACT does not use its own members' content in this respect and FACT is never the original source of the content; it will only use content that is already being illegally distributed. The team also occasionally participates in law enforcement raids to provide technical advice to partner agencies.

Additional Functions

Further to the work of the core teams as summarised above, FACT has a range of additional operational functions. These include a small forensic examinations team, which conducts IT forensics work in support of cases. This team will go out on police raids and advise on what hardware to seize, conducts examination of seized devices and produces evidential reports on the content of hard drives and other equipment (CS/05, CS/13). FACT employs a Market Strategist who focuses on hard goods being sold at markets and car boot sales. This role is highly collaborative, working closely with a multi-agency enforcement group, called the National Markets Group, which targets not only sellers but also the organisers and owners of markets where sale of counterfeit goods is a problem. Attached to the Investigations Team is a Theatrical Sector Investigator who works closely with cinemas to provide training to cinema staff and focus on enforcement activities at this point in the infringement life cycle, when people illegally use video cameras and audio recorders within cinemas. A reward scheme is in place to encourage cinema staff to be vigilant and report this type of activity. Other active operational functions include an Internet Service Provider Liaison Officer, and the certification scheme. Additionally, there are a number of support functions and roles, including administrative staff, legal counsel and a Director of Communications, who manages FACT's media and public profile.

Evaluation

FACT's model as an information and intelligence sharing organisation is well designed and implemented and, most importantly, has been demonstrated to be effective. As such, it is a model from which other organisations could learn and adapt to their own circumstances. Central to the FACT model is a commitment to being intelligence-led. It has invested heavily in its intelligence unit, which feeds into all other operational teams. This is staffed by well-trained and skilled intelligence specialists, and utilises industry standard tools. A second key principle is that it is maintains high standards in terms of the intelligence products that it produces, recognising that this is key to ensuring that partner agencies will understand and trust these products and will be able to act upon them. While there is no legal requirement

to do so, it aligns its operations to the predominant national standards – NIM and Management of Police Information [MOPI] – as this further enables its partners to understand the intelligence products that it produces and be able to trust and place reliance on how FACT handles intelligence. It formalises its relationships through intelligence sharing agreements and has these in place with multiple agencies, including most UK police forces. It is actively engaged in the relationships that it maintains and recognises and accepts that, in many instances, most of the time it will be feeding intelligence out to other organisations rather than receiving it back. It also works to improve awareness and understanding amongst partners of the legal and technical aspects of IP crime by providing training and education; this improves both the quality of intelligence that it receives from them, and increases their capability to take up FACT cases for intervention and enforcement.

In terms of how the success of FACT's information and intelligence sharing relationships can be evaluated, this study did not seek quantitative data that can indicate the number or percentage of cases or interventions that relied on collaboration with FACT's partners. However, the success of the organisation and the importance of the collaborative nature of its approach are closely intertwined. The majority of the 553 successful prosecutions in 2009 will have relied on some form of information or intelligence sharing at one or more stages in the investigation life cycle. This will be either from receipt of initial intelligence from partners at inception or during the investigation, to the provision of investigation and intelligence packages to law enforcement partners at the end of FACT's investigation in order to seek their assistance in taking the matter forward for prosecution as well as, in some instances, supplying analyses and products such as i2 charts to present in court. While FACT does pursue some private prosecutions, these can be very expensive and are only pursued in exceptional circumstances.

Of equal importance in evaluating the centrality of information and intelligence sharing in FACT's success is the testimony of its staff and officers in this respect. Many FACT interviewees discussed how it is an intelligence-led organisation, with all investigations and interventions based on the intelligence received and developed. CS/11 advised that the relationships are there, and work, because FACT needs other organisations, such as its law enforcement partners, to do things that it cannot do itself, such as financial investigation. Conversely, some of FACT's partners need FACT to undertake tasks that they can't, whilst other partnerships are based on joint interests in intellectual property crime. All of the officers, and the intelligence analysts,

within FACT stressed the reliance on effective relationships to the fulfilment of its mission:

> CS/11: “And, of course, if we can’t share anything at all as a trade organisation it’s a disaster for us. It’s a potential disaster. That’s why our partnership working is so vital to us…”

> CS/17: “So the relationships are absolutely key, and FACT wouldn’t be half as successful if they didn’t have those.”

> CS/24: “But a large proportion of our work involves preparing high quality intelligence products to take to share that information potentially with other organisations so that – hopefully – it fits within their priorities and they will take on a subsequent criminal investigation.”

There are some aspects of the model that may not be as widely translatable to other organisations. Firstly, FACT's general focus on hiring ex-police staff may not be appropriate for all organisations, and would place restrictions on the pool of potential candidates that they might otherwise recruit from. While former law enforcement officers speak the language of law enforcement, and may have a good understanding of the NIM, many are likely to lack commercial experience and may not appreciate the outlook and realities of the business world, which may hinder anti-crime and intelligence sharing efforts in the private sector environment. They may not speak the language of their peers in the business community with whom their organisations may need to establish information sharing relationships. Secondly, FACT as an organisation is entirely geared to investigation work. Other than the largest organisations, most companies will not have the resources to fund a dedicated intelligence unit within their anti-fraud units. This could restrict the extent to which the model can be replicated elsewhere.

Summary

As a non-profit organisation, FACT exists to serve its membership’s interests with respect to pursuing investigations and sanctions relating to criminal infringement of their intellectual property. It is an intelligence-led organisation, with its operational structure built around its intelligence unit. It works closely with partners in the law enforcement arena and other agencies, with the effectiveness of these partnerships seen as essential to its success. FACT implements a number of strategies and tactics

to ensure that its relationships are successful and productive. These include aligning its intelligence handling and dissemination processes with the NIM standard, adhering to the legal standards that apply to law enforcement bodies in respect of its investigative activities regardless of whether or not it is legally required to do so, and by placing emphasis on the quality of the products that it produces and disseminates.

In the next chapter, these and other strategies employed by FACT and other organisations that participated in the research will be examined in order to identify how organisations that are effective in sharing information and intelligence achieve this.

Chapter Six

Findings: Strategies to Enable Information Sharing

Introduction

Organisations share information for a variety of reasons. Some seek to collaborate with others after experiencing a fraud incident, which provided the required catalyst to take action (RI/17). Some will do so in recognition that working together is a more effective way of dealing with crime issues, seeing the big picture (CS/11, RI/15). Others may encounter an entirely new type of fraud problem and will recognise that it cannot be effectively tackled without collaboration (RI/17). Regardless of the initial stimulus, the challenges to collaboration are significant and complex. This chapter sets out some of the key findings in respect of strategies and solutions to enable and facilitate information and intelligence sharing as reported by participants, and will examine key facets of these approaches which help to make effective collaboration possible. This follows four themes. The first examines the issue of standards and the quality of intelligence. Secondly, evidence on the role of information sharing agreements and the structure of these shall be summarised. Findings will then be reported in respect of the maintenance of relationships, including the issue of asymmetrical information flow. Finally, findings relating to mass dissemination of information will be reviewed.

Standards and Quality

In Chapter Five, the importance to FACT of conducting its work in alignment with national standards and legislation was established. This strategy was also adopted by a number of other participating organisations. While not all aspects of the NIM are necessarily transferable, or desirable, for many private sector scenarios, the 5x5x5 intelligence grading system did have plenty of adherents.

> RI/07: “We always follow the National Intelligence Model in respect of the 5x5x5 evaluation process. So if we ever share information and intelligence it’s always graded and rated in that way. And that’s generally the best practice in the industry. So you would get, usually, some version of an intelligence form, which would be the 5x5x5 assessment.”

Others, including both private and public sector participants, also used the 5x5x5 grading system (RI/03, RI/06, RI/07, RI/12, RI/14, RI/15, RI/17B, RI/19A, RI/20, RI/21, RI/22). RI/14 suggested that his organisation would not use it in all circumstances, but would when dealing with law enforcement because they will understand it, whereas not everyone would:

> RI/14: "We don't do 5x5x5 with other banks because 1) the other banks probably don't understand it, though some of them do. […] If we generate, we do it all the time, logs to the police, we will follow the 5x5x5 because obviously you've got some control over, obviously, who sees that and the identity of the source and the quality of the information. So yeah, the 5x5x5 is very useful."

While several participants, including several FACT interviewees, stressed the credibility of the 5x5x5 system when dealing with police, for their part some law enforcement participants were willing to look beyond this in order to encourage referrals.

> RI/11: "We've made it too difficult for people to engage with us, because in reality why have we not just got if you want to tell me something send me an email with all the details on it and I'll convert it into a 5x5x5 with that as the source information."

RI/09 agreed, as did RI/12 – the coordinator of a cross-sector intelligence sharing scheme that includes law enforcement – who suggested that his scheme would conduct the evaluation itself on incoming intelligence. RI/09 observed that when private sector bodies employed ex-police staff in relevant roles this would often result in them adopting the 5x5x5 process.

RI/14 suggested that it would be beneficial if the process became an industry standard:

> RI/14: "And it goes back to, Carl, the 5x5x5 which underpins it. And I suppose if the banks were to use that and adopt it, or some sort of process of data evaluation and what credence do you apply to it, then I think that would feel a lot more comfortable. Because I don't want to know that you were the source, all I want to know that you're an A or a B. If you're an E or something then we

know you can't be judged. So it's giving you the comfort that when that intelligence comes to you well, it's been graded appropriately."

While many of the participants were convinced of the benefits of organisations adopting the NIM or MOPI standards (CS/18, RI20), there is no underlying national standard that applies across sectors. This itself was a significant issue for some participants. RI/10 and RI/13 were especially critical about the UK's lack of intelligence or procurement strategy, resulting in no shared standards for intelligence handling or processing, and an ongoing situation where public sector organisations often cannot open shared files due to system incompatibility. RI/10 and RI/11 also expressed concerns about the governments' failure to plan in this way. Despite this, a couple of participants did describe slow moves towards adopting industry standards. In the insurance sector, RI/19A suggested that her organisation was planning to adopt the same intelligence database used by RI/03 as this was the industry standard. In the public sector, RI/20 and RI/21 explained that their organisation had adopted the Trading Standards' database so that Trading Standards officers would have access to their organisations' intelligence, with appropriate safeguards, and that they were moving to allow joint access:

RI/21: "…we're at the stages now of moving towards a situation where properly accredited people working for Trading Standards can directly access our data. Equally properly authorised people in ours can access directly Trading Standards' data."

Due to the emphasis placed on aligning with legislative or law enforcement standards, several participants referred to processes being in place to review the quality of both incoming and outgoing information (CS/04, CS/17, CS/21, RI/01, RI/06, RI/09, RI/18). Adherence to accepted standards, and having a reputation for producing high quality and reliable products and intelligence, are essential components of effective collaborative relationships (CS/24).

Information Sharing Agreements

One commonly used tool by which to agree standards, and to help structure and formalise a collaborative relationship, is an information sharing agreement, or memorandum of understanding [MOU]. These documents can take many forms, and the precise structure and content vary according to each individual information

sharing relationship. However, their primary purpose is to set out and formalise the agreed basis on which partners will share data, information or intelligence.

MOUs were a common topic of discussion during interviews across both phases of data collection. They formed a central part of the information sharing strategy of several participating organisations. At least twelve FACT interviewees discussed the role and utility of MOUs in facilitating intelligence sharing. FACT uses MOUs extensively with its partners; CS/23 stated that FACT has MOUs in place with most police forces, with all of the GAIN networks and with other agencies. The MOU is seen as central to FACT's ability to collaborate with others and to demonstrate to partners that it works to appropriate standards:

> CS/18: “It's building confidence into those documents, and that takes a number of forms. The biggest one is probably data protection. They've got to understand, our partner agencies don't have to work with us really, they don't have to give us information, so they need to understand that when they do agree to share information with use that we deal with it in a professional and legitimate manner [...] the MOU is the thing that gives us the opportunity to work together...”

Other participants also referred to regular use of MOUs in framing and managing their intelligence sharing relationships, with RI/01, RI/03, RI/08, RI/09, RI/11, RI/12, RI/13, RI/17, RI/18, RI/19A, RI/20 and RI/21 discussing how their organisations had agreements in place. As would be expected, the extent to which these were used varied, with some interviewees stating that their organisations had agreements in place for every intelligence sharing relationship that they had, while others were for use with specific partners or sectors. For RI/11, who worked in a law enforcement body, they are not needed for sharing intelligence with other law enforcement agencies, but were with industry:

> RI/11: “We’ve got and we use SLAs [Service Level Agreements] in terms of all this. I mean, when it comes to the general intel within law enforcement then no, because we don’t need that because the MOPI and NIM and everything like that. When it comes to the outside agencies then yes, we have MOUs and SLAs.”

Some participants suggested that a similar affinity-based approach may be used within certain industries and sectors. RI/19A, an insurer, suggested that her organisation has MOUs in place directly with some police forces, with other bodies through a collective MOU maintained by an insurance industry fraud intelligence sharing scheme, but when sharing information with other insurers they would rely solely on the DPA s.29(3) exemption. RI/20, the Head of Intelligence in a public sector organisation, suggested that his organisation didn't need MOUs when dealing with other public sector bodies, but does have a standard agreement for use with industry partners. However, while the experience of many participants suggested that they favoured the use of MOUs, it was noted that these merely helped to structure the workings of a relationship and still relied on legal channels to share being in place; they do not enable intelligence sharing in their own right.

> CS/22: "…the statutory gateway's there; an MOU only goes a little bit further. Well, actually, not really further at all but saying what can and can't be done. It's just that, really, an understanding to help understand the legislation and the relationship […] So the statutory gateway says that it can be done; the MOUs specify how it will be done."

MOUs do have drawbacks, however. Several participants pointed out that they can be time consuming to put together, with time frames cited between three and six months (CS/11), six to twelve months (RI/11) and, at the most extreme end, two to six years (RI/02). The volume of paperwork required if an organisation were to have agreements in place with every organisation with which it had an information sharing relationship was also mentioned as a factor (RI/06). Furthermore, the level of complexity in the agreements increased with the number of parties involved, and all aspects need to be agreed by all parties. One participant (RI/18), who had been working for a law enforcement agency on an overarching framework of cross-sector agreements with multiple partners, described a situation where multiple levels of MOU had to be completed. Three protocols were agreed through various stages of piloting and prototyping of arrangements, with a fourth agreement to be put in place after completion of the initial trials. These issues can be problematic, but RI/13 argued at length that this need not necessarily be the case. He put forth a strong case that it should be possible to achieve, in the public sector at least, just a handful of agreements based on general principles that should cover most agencies in most situations, and that this should be done at higher levels rather than each individual agency having separate agreements in place:

> RI/13: “If you take the Prison Service and Law Enforcement: there’s 4 information sharing agreements between those agencies, on corruption and general information and probation-led information. Why do you need 4? So on paper it works, or does it? And not only does it have 4 national ones, but there are regional information sharing agreements between Prison Service and..., and there are local... Why? Why are we doing that? Why don’t we have one overarching information sharing agreement that is drafted in a way which allows for the flow of information?
> […]
> There are 203,000 police staff, police offers and PCSOs [Police Community Support Officers] in policing. At the very least you can have an information sharing agreement between them and NOMS [National Offender Management Service]. We don’t need 43 forces doing that. We don’t need dozens of local, everywhere where there’s a prison, there’s an information sharing agreement with that local BCU [Basic Command Unit]. We don’t need that.”

Not all organisations, or information sharing models, rely wholly on MOUs. Several participants, representing industry-based anti-fraud information sharing schemes, avoided the need to have individual agreements in place with each member by incorporating the fundamental elements of these within the membership contract and terms of reference (RI/03, RI/04, RI/06, RI/15, RI/17B). This approach represents not a rejection of the MOU, but an alternative to it, and resolves the problem of having multiple unique arrangements in place. This helps schemes following this model to avoid being undermined by complexity, but the rigidity means that agreements cannot be tailored to suit all organisations; those that do not agree to the standard terms would not join as members. Even these schemes sometimes make use of MOUs with other sectors, however, for the benefit of all members (RI/19A). Others will also make use of, where held, their SAFO status to enable cross-sector sharing by encouraging public sector organisations to join and collaborate with the scheme on the strength of the assurances provided by that designation (RI/06).

However, some organisations proceed without the use of MOUs altogether. RI/07 and RI/14, representing investment and retail banks respectively, suggested that they do not have formalised agreements in place, but rely on informal, ad-hoc arrangements utilising the DPA s.29(3) exemption on disclosure. This is, perhaps,

especially notable given that the financial services sector was the sector most commonly cited by participants as being effective at sharing anti-fraud information.

Structure of MOUs

During the case study research, FACT provided a copy of its standard MOU template for examination, as well as copies of three signed agreements: one of which was based on the FACT template, and two with police forces using those organisations' agreements (FACT, 2008; City of London Police, 2012; Metropolitan Police, 2012).

While the structure, length and organisation of the documents differed quite considerably, some common features of all three are set out in Figure 6.1.

Figure 6.1: Common features of information sharing agreements

Key Element	Types of Content
Purpose of the agreement	What participating organisations will seek to achieve through collaboration
Information on participating organisations	Details ranging from organisation name, SPOCs, key officers, organisation's missions and focus
Nature and type of information to be shared	Outline of the purpose for sharing the information
Key principles underlying the agreement	Lawful exchange of data; defined purposes of crime prevention, detection and investigation; relevant codes of practice (e.g. MOPI)
Legal basis and channels for sharing	Data Protection Act (referred to in various levels of detail); s.29(3) requests; MOPI
Intelligence handling and assessment	5x5x5 handling codes; information security; usage of data; retention and deletion of data
Mechanics of sharing	Forms; communications channels (e.g. secure email addresses)
Signatures	Signatures of responsible officers; commitment to abide by terms of agreement; provisions for monitoring and review

There were also a number of features within the documents that were not necessarily common to all three, but were still potentially helpful elements, as detailed in Figure 6.2.

Figure 6.2: Useful additional features within information sharing agreements

Key Element	Additional Detail
Definitions of key terms	Examples: 'information sharing'; 'data'; 'intelligence'; 'information'; 'data controller'; 'policing purpose'
Benefits of the agreement	Benefits for each party; public interest benefit
Complaints procedure	Outlines the process for handling issues and problems arising within the agreement and relationship
Audit	Outlines requirement for decisions to be documented and auditable
Sharing personal information	Explicitly deals with issue of sharing personal information, and why this may be in the public interest to do so
Time frame	Establishes time parameters for providing responses to information requests for standard and urgent enquiries

Audit and Compliance

A feature that some organisations and information sharing schemes incorporate into their collaborative arrangements is the right to audit partners on their adherence to the terms of their agreements. As would perhaps be expected, this feature was especially prominent amongst the membership schemes that exist to enable anti-fraud information sharing, such as those represented by RI/04, RI/06 and RI/17B, the latter of which confirmed that her organisation performs biennial audits on each member. The right to perform audits is built into the membership agreements of these schemes. If members are found not be adhering to their contractual obligations, sanctions – such as the cessation of membership – may be imposed. This can help schemes to ensure not only that members are adhering to required standards, but also that they are providers as well as recipients of information to help overcome the issue of asymmetrical flow of data. RI/15 represents another industry-based scheme, but with a very small staff, and there is no formal audit process in place. However, RI/15 did describe how he will take up directly with members their failure to share relevant information or to fulfil the obligations to which they had signed up.

RI/20, representing a government agency, also referred to auditing processes with partners. Its MOUs require partners to acknowledge MOPI standards and the NIM,

and to be subject to the oversight of relevant regulatory bodies, such as the Surveillance Commissioner and the Criminal Case Law Review Commission, to which RI/20's organisation is accountable. Some participants referred to being audited by regulators as a standard process, with RI/06 stating that his organisation had been notified of an imminent audit by the ICO and that they had no apprehension about this due to the standards and processes that were in place and due to previous experiences of such audits. Others, including RI/01, RI/04, RI/17A, RI/17B, RI/18 and RI/19A, discussed the merits of ongoing dialogue with the regulators, while RI/08, who worked for a regulatory body, discussed active engagement with organisations to promote compliance and provide advice.

DPA s.29(3) Requests

Central to many of the participants' strategies for sharing information with other organisations, whether as part of a data sharing scheme or a bipartite relationship, was the DPA s.29(3) exemption. This allows sharing of personal data for the prevention and detection of crime or the apprehension or prosecution of offenders where the failure to share this data would be likely to prejudice these purposes (ICO, 2001, pp.42-43). While this is an exemption from the restrictions on sharing, rather than a gateway to facilitate exchange, this is an important tool for those seeking to share economic crime intelligence. All three of the MOUs provided by FACT made explicit reference to the provision, while the Request for Information form appended to FACT's template specified this as being the legal basis upon which data was to be requested. Other participants discussed the provision extensively as being important to their organisations' intelligence sharing relationships, regardless of whether or not they used MOUs. Several FACT interviewees discussed the channel, including CS/1, CS/16, CS/18, CS/23 and CS/24, as did non-FACT participants RI/01, RI/03, RI/06, RI/07, RI/09, RI/12, RI/14, RI/15, RI/17A, RI/18, RI/19A, RI/19B and RI/20. For all of the problems that the DPA can cause – outlined in Chapter Four – there was widespread appreciation for the way that the exemption is structured when used properly:

> RI02: "I think the Data Protection Act is appropriate for the thing that it's there for. The problem is how it gets used in order to ensure that personal identifiable data is shared appropriately and I think the way that it's done in the Data Protection Act is great."

> RI03: “I actually think 29(3) works pretty effectively, to be perfectly honest with you. I think if you understand the legislation, if you engage with the regulators, if you operate a sound business model with good governance and you have proper controls around it, then I think 29(3) as it stands already provides a good framework.”

Whilst it remains a misunderstood, and often misinterpreted channel, if used appropriately the DPA can be an effective facilitator of intelligence sharing for anti-fraud purposes, as attested by the participants in the study.

Building and Maintaining Relationships and Networks

The establishment and maintenance of relationships is, unsurprisingly, essential to successful collaboration. Many elements of the interviews focused, both directly and indirectly, on how participants and the organisations they represented went about ensuring healthy and productive information sharing relationships with partners. A number of key topics, strategies and factors emerged, of which some of the primary subjects are discussed below.

Information Asymmetry and Reciprocity

The flow of information in only one direction between organisations has been well recognised and documented as an issue, as people are typically more interested in receiving information than providing it (Bharosa et al, 2010, p.63). This emerged as a significant problem by participants within this research too, as reported in Chapter Four. There were a number of responses and strategies discussed with respect to this issue, and reciprocity was identified as a key principle for maintaining effective collaboration (RI/03, RI/04, RI/05, RI/06, RI/11, RI/14, RI/17B). Some interviewees representing industry-specific intelligence sharing schemes (RI/03, RI/04, RI/06, RI/17B) stated that it was such an important element that it was built into the contractual obligations of members to actively provide, as well as request and receive, relevant data, and this was subject to audit as discussed above. While some participants also discussed hopes that their organisations’ SAFO status might help in this respect when sharing with the public sector, both RI/15 and RI/17B suggested that they had experienced continued resistance from some bodies, such as HMRC, after they became SAFOs and that many public sector organisations still did not know what the status signified. RI/04 suggested that her organisation had enjoyed some success by accepting public sector organisations as members of its scheme. Furthermore, she described how her organisation periodically arranged round table

discussions as part of the work of a sub-group, and had found that bodies such as HMRC and law enforcement were engaging more through these fora. RI/21, representing a public sector body, reported that his organisation had managed to break down some of the barriers with respect to HMRC and the Border Agency due to the strength of relationships forged with some of the HMRC policy officers that also worked with that agency. However, he still found the results inconsistent, in that some HMRC officers would share intelligence with him on provision of a DPA s.29(3) request form, whereas others would not.

For FACT, two primary strategies to this issue emerged from the data. The first was the importance of agreeing common goals and each party's responsibilities on a case-by-case basis, an approach also agreed by RI/05. The second was to accept that most information would be likely to flow in one direction:

> CS/18: "…for years now the government have been saying 'public-private partnerships are the way forward' – but they've never told you how you're meant to do that. So we say 'this is how we think we can do this, because we can't work together unless we share information'. And we decide on common goals, and we decide on a particular case who's going to do what. So that all works very, very well. What we do know, and what we say when we're doing it, is we realise that as a public organisation the chances are that you're going to get a lot more information out of us than we're going to get out of you. But we accept that."

This philosophy was shared by RI/20, who was willing to share regardless of what he received back on the basis that the information shared would be likely to spur action taken by other organisations and it was thus in his interest to do so:

> RI/20: "Doesn't make it difficult for me, I share unilaterally. If they don't care to share back, that's more their problem than mine."

However, it remains a contentious issue, with inconsistencies in the approaches of people within the same organisations. RI/21, who works in the same organisation as RI/20, suggested that non-reciprocation can only go so far before it becomes a problem, and CS/22, amongst others within FACT, expressed frustration at not receiving much back.

Reputation

Other vital attributes in both establishing and maintaining productive information sharing relationships are those of trust and of having a reputation as an organisation that produces high quality work and which can be relied upon to handle intelligence and sensitive data appropriately. Trust and reputation were widely cited, especially amongst FACT participants, as being critical to the success of partnerships. Eleven FACT interviewees, including its three most senior officers, considered FACT's reputation for quality and competence to be key to collaboration.

> CS/24: "I think that the fact that you get a reputation for providing high quality products. Without a doubt that is key. We frequently do get flagged up by people, you know 'I wish everybody did intelligence like FACT'. It is that reputation side of things."
>
> RI/14: "And what underpins everything is trust."
>
> RI/19A: "Because it's about trust. It's knowing that when you share that intelligence that you know the parties that you're sharing that intelligence with are going to deal with it compliantly, they're going to store it safely and they're not going to bring you issue for releasing it in the first place."

Trust and reputation were identified as fundamental elements by numerous participants, and cited as essential by eleven interviewees in the second phase of the research, while lack of trust was also identified as a barrier to collaboration by another (RI/10).

Personal Contacts and Networks

It became clear from many participants that the basis of trust can rely significantly on the personal relationships, networks and, often, the history and background of people actively involved in the sharing of information. This took two main forms.

One was reliance on the normal relationships built up between practitioners, often originally built through networking events such as conferences, industry events and industry peer networks (RI/01, RI/05, RI/07, RI/10, RI/11, RI/19A, RI/21). RI/15, who was newly in post as the Chief Executive Officer of an intelligence sharing scheme,

discussed having inherited ‘established trust’ within the network and of the need to maintain that.

The second form was a reliance on the networks of practitioners from their previous careers in law enforcement or the military, where the underlying basis of trust is built on shared backgrounds, common interpretation of standards and mutual understanding. This was discussed especially by five participants (CS/18, CS/22, RI/01, RI/07, RI/14) as being an important aspect of establishing networks and trust. For FACT, CS/22 suggested that a significant number of staff were ex-law enforcement officers and that this helped them to establish relationships with ex-police officers working in other organisations. RI/14, who described it as “the old boys club of law enforcement”, suggested it was a system that works.

Regardless of the underlying basis of the personal relationships that are established, they can be important factors in facilitating exchange of information as that is where the trust in the standards and competence of collaborating partners is shown:

> RI/19A: “I have much more confidence in sharing intel with people I know, I know almost on a personal level, because I know I can trust them, I know they have the same work ethics as us. Similar processes, controls.”

Informal Channels of Communication

Taking the subject of personal relationships and networks one step further, it also became apparent in a number of the interviews that reliance was placed by some organisations on relatively informal channels of communication between the personnel involved. This was often in the form of initial, undocumented, conversations which may, or may not, be followed up with a formal recorded request. Several interviewees discussed this type of informal or off-record discussion (CS/24, RI/05, RI/07, RI/13, RI/14, RI/19A).

> CS/24: “…there are occasions where people want to talk to you on the record and off the record. And from an intelligence perspective you have to have that. There’s nothing wrong with that, everybody understands that there are these occasions when that is required.”

> RI/05: "…we'll speak to IFED [Insurance Fraud Enforcement Department] and we'll generally get off-the-record steer about whether or not they're going to do something or not going to do something."

Some such exchanges were described by participants as a preliminary discussion, to establish the nature of a request and identify if there is relevant intelligence to share, followed by submission of a formalised request by one of the parties (RI/07, RI/19A). Other participants discussed some situations in which off-record approaches were seen as necessary in order to bypass or evade rules or regulations (RI/07, RI/13, RI/14).

> RI/07: "So as well as thinking about the external framework, we've got our own internal controls and monitoring so that's something that some people might thing 'God, it's not worth my while to try and send that out because I'm just going to get flagged up for doing this and doing that and I'm going to get in trouble for it and actually, I'll just pick up the phone and tell them.'"

> RI/14: "If I know the police officer, I'm mindful of the fact that if I respond to s.28 [sic] I'm the data owner and I can do that. However it may not be in the interest of our customers. So very often I will say to the police officer I'll give you this for intelligence purposes, however if you want to produce it lawfully you have to get a court order."

Such tactics are akin to those described by Handy (1993, p.308) as informal channels or cliques used in a manner to bypass rules in order to achieve required outcomes.

Other uses of informal channels were to give other organisations or contacts an early warning about trends or issues. RI/07 described how her organisation might call contacts to share general information about potential criminal activity, but would make it clear that it was unconfirmed intelligence provided for general awareness purposes.

Onward Referral and Indirect Sharing of Intelligence

Data ownership was an important consideration discussed by many participants in both phases of data collection. Linked to issues of trust and competence in intelligence handling, as well as important in respect of data protection legislation, ownership affects organisations' ability to disseminate information to, and receive it from, others. The underlying principle is that if an organisation doesn't own the data,

it cannot share it without relevant permissions from the owner. This precept was accepted and recognised, either implicitly or explicitly, by all participants in the research, and there were two main approaches discussed in how to deal with this issue.

The most common response to this type of scenario would be that of onward referral, or signposting. One organisation which has, or is aware of, intelligence required by a partner would not share it directly with that partner, but would refer them to the data owner in order that they could request it directly (CS/04, CS/11, CS/18, CS/23, CS/24, RI/05, RI/06, RI/12, RI/15, RI/17B, RI/22). It would then be up to the data owner to determine whether they wished to collaborate with the requester. Some information sharing schemes are organised in a hub-and-spoke structure in order to facilitate sharing in this way, with the scheme acting as the conduit through which requests and responses are channelled (RI/12, RI/15). Several participants (RI/06, RI/15, RI/17B) suggested that their organisations might facilitate the discussion if needed. Another option was for the organisation holding another's intelligence to request permission from the data owner themselves to share it onwards (CS/18, CS/22, RI/12).

Taking this a step further, the second tactic used by a couple of organisations, including FACT, was to leverage the strength of an existing intelligence sharing relationship to enlist the partner organisation to seek intelligence from a third organisation on its behalf.

> CS/24: "The other thing about [partner agency] is they have the facility to obtain intelligence from other agencies that we, FACT, would not be able to speak to directly. So the likes of PayPal, EBay, some of the other payment processors, etc. And we have a referral process where we can make requests for information from them. It's really so useful because they can give us that data."

RI/22 suggested a slightly different arrangement available to her law enforcement agency, in which it could utilise the Europol forum to obtain material in respect of Russia when it would not be able to obtain that data directly from Russia itself. While this particular facility would not be available to non-law enforcement organisations, the principle is similar to the arrangement discussed by CS/24 as noted above.

Single Points of Contact

One of the tools used by many organisations to facilitate collaboration – and as the mechanism by which trust is established, standards upheld, communications channels directed and relationships maintained – is the Single Point of Contact [SPOC]. These are used extensively by FACT, and by several other participants, including RI/03, RI/05, RI/06, RI/07, RI/09, RI/15, RI/18 and RI/19. RI/06 noted the incongruous nature of the term as there were often multiple SPOCs in place in a relationship. He also reported that the data sharing scheme that he represented has documented guidance on the SPOC 'Role Profile' and 'Roles and Responsibilities' to which all members sign up, such is the importance of the position. Where they are used, SPOCs are seen as the owners or gatekeepers of the relationship, and are often identified by name within MOUs.

Pilot Projects and Joint Working

Several participants (RI/01, RI/02, RI/03, RI/04, RI/17B, RI/18) discussed the use of trial projects, or pilot schemes, as a means to test the potential for a collaborative venture. As well as providing evidence for further development and wider implementation (RI/02), if the pilot demonstrates positive results it can also help to develop mutual understanding between partners. Similarly, joint working on projects, such as FACT co-authoring a jointly branded report on illegal streaming with the NFIB (CS/22), was also cited as good means to develop and strengthen working relationships. Other participants also provided examples of collaborative projects, investigations and enforcement action (RI/03, RI/12). Participating in, or organising, working groups between multiple collaborators was also reported to be a positive strategy to foster cooperation and develop mutual understanding and trust (CS/06, CS/19, RI/04, RI/05, RI/18, RI/19A). RI/09 and RI/14 discussed how their organisations also made use of staff secondments to strengthen collaboration and cement understanding with partners.

Senior Level Involvement

Securing the involvement and support of senior level executives was generally recognised to be important in ensuring both the success of a collaborative scheme or project and in strengthening the information sharing relationship between organisations. This was seen as important in terms of enhancing mutual understanding and, essentially, in helping to drive and, where necessary, change corporate culture in favour of information sharing (RI/03, RI/15, RI/17A, RI/19A). CS/24 and RI/14 both stressed the value of having decision makers on board and,

ideally, involved in key meetings to ensure that participants can make commitments on behalf of their organisations. Failure to empower representatives leads to frustration and delays. CS/18 discussed how gaining the support of senior officials, such as police Chief Constables, can help gain traction and ensure that action is taken. The involvement of senior officials can provide reassurance to both parties of high level control in the processes and relationship (RI/05). To this end, RI/03 described how his organisation actively decided to change the composition of the board from fraud managers from member organisations to executives who could make strategic decisions and agree budgetary commitments.

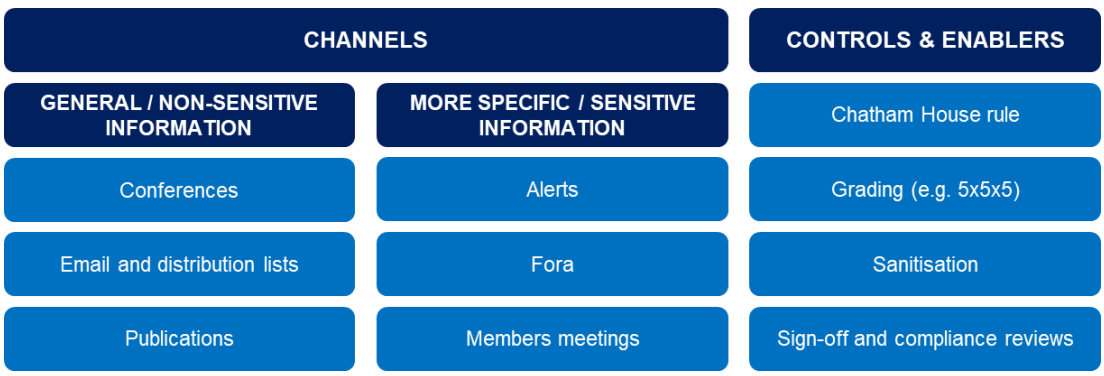
RI/02, representing a government department overseeing a number of anti-fraud intelligence sharing projects, stated that there was substantial senior level buy-in within and outside of government. However, RI/06 suggested that this was not always the case, citing senior HMRC officials still failing to recognise the operational benefits of information sharing, despite ground level staff doing so.

Mass Dissemination of Intelligence

Many of the matters outlined above are concerned primarily with dissemination of information on a one-to-one basis. However, there remains a need in many respects for anti-crime information to be broadcast at a wider level, on a one-to-many or many-to-many basis. In many instances this will not necessarily entail the sharing of personal or sensitive information, although in some it may. This section provides a summary of some approaches discussed by participants in respect of these needs.

The primary methods discussed during the interview with respect to mass dissemination are outlined in Figure 6.3.

Figure 6.3: Channels and controls for mass dissemination



For generalised information and intelligence, publications (CS/18, RI/04, RI/07, RI/17B, RI/10), conferences and fora (CS/01, CS/05, CS/18, RI/04, RI/06, RI/07, RI/11, RI/14, RI/22) can be effective means of mass collaboration, and especially useful for sharing information such as trends, issues of general interest and applicability, case studies and techniques for detection, disruption and enforcement. Conferences and other fora also provide valuable networking opportunities, which may help delegates build and strengthen relationships with others facing similar challenges and risks (RI/07, RI/14, RI/19A). The nature and content of publications may range from newsletters, reports and analyses of fraud issues to detailed Strategic Assessments as produced by FACT. Online publications and fora such as fraud wikis were also lauded as creating opportunities for exchange through the creation of open repositories for anti-crime information (RI/10). Email exchange was considered by some to be an effective tool for disseminating information on a mass basis, as well as for sharing data files on a one-to-one basis, and thus as a useful facilitator of intelligence sharing (RI/06, RI/11, RI/19A). Email could, however, present challenges of its own, from restrictions on attachment sizes to messages being blocked by firewalls and security software at the end of either the originator or the recipient (RI/07, RI/11, RI/14, RI/18).

For more sensitive information, or debate of issues specific to defined groups, such as industry peers (for which tension exists between sharing and competitive advantage), more defined fora, members meetings of intelligence sharing schemes and special interest groups may be more appropriate options. Several participants, including CS/18, RI/06, RI/12, RI/15, RI/17B and RI/19A, discussed such events for purposes ranging from the discussion of general trends through to frank dialogue about sensitive issues behind closed doors. In order to promote openness, conventions such as the Chatham House Rule can be observed to enable debate of details that would otherwise not be shared between separate, often competing, entities (RI/07, RI/14, RI/19A).

Issuing alerts was another commonly discussed method of sharing both general non-sensitive information (RI/04, RI/09, RI/11, RI/18) to more specific actionable intelligence (RI/06, RI/07, RI/09, RI/14, RI/17A), with controls and restrictions being placed on the latter. For the intelligence sharing scheme represented by RI/06, e-alerts were the primary means by which members would share intelligence, and these are posted onto the scheme's website where they can be searched by other members. The scheme emails notifications to members when items of potential

relevance or interest have been made available to search. Additional controls are applied, including grading alerts using the 5x5x5 system. Furthermore, the alert being posted would be signed off by that organisation's registered SPOC, and would be reviewed by the scheme's compliance officers (of which RI/06 was one).

An additional technique discussed by several interviewees as a means of enabling large scale dissemination of anti-fraud information was data sanitisation. Anonymisation and pseudonymisation of otherwise sensitive data may render it suitable for sharing with a wider audience than would otherwise be possible or legal (RI/07. RI/08, RI/10, RI/15). In its Code of Practice on anonymisation, the ICO makes it clear that statutory data protection constraints do not apply to anonymised data where the data subject is not identifiable (ICO, 2012, p.7). Such treatment was also reported to be beneficial in overcoming potential uncertainty over a recipient's ability to handle intelligence appropriately (RI/22), and in transmitting intelligence internally within organisations across territories with strict rules on transmitting sensitive data (RI/07).

Summary

In this chapter, findings relating to some key facilitators and enablers of intelligence sharing, and characteristics of collaborative relationships, have been set out. The topic of establishing and adhering to acknowledged standards has been covered, with many participants considering this helpful in enabling intelligence sharing, but others not considering it essential. Likewise, many organisations and intelligence sharing schemes define standards and processes within MOUs or contracts, whilst others are content to rely on formal requests made under DPA exemptions. Factors such as trust and reputation for competence in handling intelligence were found to be integral to productive relationships. Conversely, there is still reliance on private networks, including amongst alumni of law enforcement bodies, in some areas to enable sharing, which restricts opportunities for sharing outside of those restrictive networks. Finally, there are techniques available to allow dissemination of sensitive information amongst many participants through appropriate sanitisation or observance of conventions such as the Chatham House Rule.

The next chapter will explore findings with respect to related issues such as competence in intelligence handling, the role of training and education, and the drive towards professionalisation in intelligence sharing.

Chapter Seven

Findings: Setting the Standard – Knowledge, Skills and Professionalisation

Introduction

Findings outlined in previous chapters have indicated that, in order to establish successful information sharing relationships, organisations and practitioners must not only have the willingness to collaborate constructively but also the understanding and skills to do so. They must also be trusted by others in these respects. This includes not only understanding the legislative and regulatory framework, but possessing the skills to handle, process and disseminate data appropriately and legally. This chapter examines findings relating to the importance of competence in intelligence handling, approaches to training and education, and in respect of a tentative emerging professionalisation agenda within the anti-fraud and intelligence communities.

Competence

The issue of competence in people's and organisations' ability to legally and appropriately handle sensitive information and intelligence was found to be of considerable concern to participants. The matter is closely connected to reputation and trust, which underpin the relationships that are essential to effective information sharing. It was a factor discussed by eleven interviewees within FACT alone as an important element in successful collaboration, as well as by four other participants as a significant issue. Lack of competence in handling intelligence correctly not only impedes information sharing, but can have damaging implications both for individual investigations and for wider collaboration prospects:

> CS/11: "We have big issues with this because obviously we work within a bigger environment – intellectual property – so anything negative that's done by anybody else rebounds very, very quickly and the doors close and people back off. So a great example would be Google. Where there isn't a point of contact for the industry as a whole. Everyone's vying, everyone's just being selfish, everyone wishes to get their stuff done and someone will drop a clanger by sending a request to Google that asks them to do something that's wrong, shouldn't be asked for. Probably illegal in the request. And so Google will take that and they will go and stand on top of their building and wave it at

> the IP industry and say 'look at this, you've made a complete hash of this, and this is why we won't be doing it anymore.' […] Huge problem for us because there's lots of individuals representing big organisations who really don't know what they're doing, pulling the wool over people's eyes, protecting their own jobs. All kinds of issues. It's a massive, massive problem for us."

Professional incompetence isn't solely restricted to errors in the processing of data or in making inappropriate or illegal requests for, or disclosures of, sensitive data. Problems can also arise with respect to inconsistent or inappropriate application of standards, such as the 5x5x5 grading process (CS/04, CS/21, CS/24, RI/21). The tendency to inundate others with requests was also cited as a significant issue by several participants.

> RI/19: "…that's a big industry problem at the moment – firing s.29s off left, right and centre without an understanding of whether it's going to be a fruitful exercise or not."

> RI/07: "I know a couple of groups did drop out of [information sharing scheme] and that's because you had a couple of companies within it who were just bombarding companies with intelligence requests and I think that was something that people get nervous about."

An alternative problem is that of excessive information being provided. RI/13 made the point that if an organisation provided a partner with intelligence in the form of a 158-page document that would likely both be excessive information and less effective in terms of actionable intelligence; in all likelihood it would not be read.

Strategies for ensuring competence link back to other processes within the relationships, including focusing on quality rather than volume (CS/24), utilising SPOCs as gatekeepers (CS/24), and agreement of processes. The latter may be achieved through MOUs and mutual understanding or through development of industry-wide standards on information requests such as the voluntary code for the insurance industry (Chartered Insurance Institute New Generation Group, 2015) cited by RI/19A and RI/19B. Many organisations also place significant emphasis on training staff in order to ensure technical proficiency.

Training and Education

An important means used by organisations to ensure that staff have sufficient skills and ability to handle and share information is by providing them with education and training. These play a vital role in facilitating collaboration, and fulfil a number of functions for organisations that are seeking to share information to combat economic crime. Not only can training and education be used to equip operational staff to process intelligence and sensitive data appropriately, but it can also be an essential tool in helping to overcome cultural barriers to information sharing (RI/01, RI/02, RI/14).

The scale of the education requirement is extensive. The need is not restricted just to fraud staff, or to employees within organisations involved, or seeking to be involved, in intelligence sharing. It extends to organisations across all sectors, to data controllers in organisations large and small (RI/01), as well as to making the case for data sharing to the general public (RI/02, RI/13, RI/18). As such, there is a role for many stakeholders, including organisations, regulators and the government, with respect to education and awareness around information sharing (RI/02).

One of the most significant educational functions discussed by participants was providing awareness training to partner organisations to enhance their understanding of the purpose of the information sharing relationship, the issues involved and the type of data that they required, as well as, in some cases, the nature of the criminality and the relevant legislation that applies (CS/22, CS/24, RI/03, RI/09, RI/15, RI/18).

> RI/03: "I wouldn't say we do training for police or regulators, I'd say we do awareness; so if we go in and speak to a new police force, we would have to make them aware of different types of fraud and how the model works. But from a data sharing point of view our engagement with police and regulators is more around explaining our rationale for wanting to share the data rather than trying to educate them how to share data."

> CS/24: "The reality is that our world has changed, our priorities have changed and we're moving very much into an online – well we are, totally focussed on the online problem – but there's still very much what we call a hard goods issue which is the sale and distribution of high quality DVDs. So we do still find that a lot of people that pass us intelligence are passing us intelligence in relation to things that we are unlikely to do a lot of work on."

By educating partners on their information requirements, organisations can help to ensure that partners understand their needs, share relevant intelligence and provide less irrelevant data, making the process more productive and efficient for both parties. FACT provides training not only to police forces on the nature of IP crime and how to respond to incidents (CS/22), but to non-law enforcement partners too. It provides training every year to Crimestoppers in order to help its staff understand FACT's information needs and obtain relevant information from people reporting IP crime to them. FACT's annual Strategic Assessment document, too, is an educational tool used to promote understanding amongst partners. Education programmes are not only useful for external awareness. RI/19A spoke of a large internal campaign conducted by her organisation to educate its insurance claims staff on what intelligence was and the benefits of it, and stated that referrals to the fraud team had increased significantly as a result.

Another key angle of the training and education agenda was providing training on intelligence handling and the core standards and processes. For RI/12, representing a cross-sector intelligence sharing scheme, it is important to do this to ensure that the organisations involved in the scheme understand what intelligence is and how they should be sharing it. To this end, his organisation provides induction training for new scheme members. Similarly, RI/06, who is on the board of an industry-based scheme, provides mandatory training for the SPOCs nominated by member firms. This involves a training day and completing a training package, covering both the NIM and the specific roles and responsibilities of the SPOC within the scheme. Until they have completed the training, they cannot undertake the SPOC role, as it is the SPOCs that sign off any intelligence sharing alerts and act as the gatekeeper from the member firm's perspective. RI/06's scheme was also investing in an e-learning package on the NIM, and had agreed to pay for scheme members to receive training from law enforcement on how to improve the quality of evidence packages supplied to the police. Other participants' organisations also provided training to members on subjects such as the NIM, the legal basis for sharing (including DPA s.29(3)) and how to handle and grade intelligence (RI/03, RI/12). RI/15, who spoke on behalf of another industry-based scheme, organises regular information sessions and workshops for members with training provided for people in different roles, such as analysts, investigators and re-sellers, as well as crime awareness programmes for the public, including a publicity campaign for young people. The training of internal staff is important too, with FACT devoting close attention to ensuring that new starters – and

all staff – receive NIM training, as well as training on the systems and processes for handling intelligence and on how to apply the 5x5x5 grading system (CS/04, CS/12).

RI/13 – who works as an intelligence lead within a police force and who has worked on intelligence-sharing projects for ACPO – suggested there was a need for greater focus on intelligence training for police officers who were not in intelligence specialisations. He pointed out that new recruits would typically receive two weeks of training on issues such as human rights, equality and diversity, which he recognised as topics worthy of training resources, but only forty-five minutes on intelligence. This subsequently caused problems for (trained) intelligence teams who would spend valuable time trying to interpret intelligence reports written by officers who are not trained to write them properly, rather than devoting this time to developing that intelligence.

Professionalising Intelligence

The discussions on competence, training and education with respect to intelligence handling and sharing inevitably led, in some of the interviews, to the topic of professionalisation of intelligence-related roles. Some interviewees within both phases of the research talked passionately about the need for professional controls, standards and recognition.

> CS/11: "I don't think the world has really got on top of information sharing at all. It's not a hugely recognised skill, and it actually is vital and should be. It should be a profession. Definitely. Definitely."

> RI/13: "I would talk about a professionalised intelligence community who have training, and a programme of continuous development, continuous professional development."

While an extended discussion of what constitutes a profession, and the changing conceptualisation of professions and professionalism, is outside of the scope of this thesis, it is worth considering briefly some of the key characteristics of professions in order to consider whether intelligence as a specialism is moving toward professionalisation. While it has been argued that it is no longer relevant to define professions by key characteristics (Evetts, 1999, pp.119-120), and that within the changing occupational environment it is difficult to define what it means to be a professional (Noordegraaf, 2007, p.781), some common attributes and qualities may

still be applied to the concept. Some of these attach esteem to the concept of professions beyond the direct technical aspect of professional endeavour (Muzio, Brock & Suddaby, p.713). Professions are founded upon a body of skill and theoretical or abstract knowledge, gained through specialised education and training, and professional work is characterised by the application of judgement (Freidson, 1989, p.425). This body of knowledge is protected, and it is the professional who has access to the monopoly exercised over that knowledge and techniques through their recognised status (De Lang, Jackling & Suwardy, 2015, p.43). The knowledge base is supported, and controlled, by an institutional framework that controls access and codifies standards, certifying members as professionals and maintaining an ethical foundation (O'Regan, 2001, pp.217-219). These are supplemented by activities including an active research agenda, a sophisticated literature and published serials or journals (O'Regan, 2001, p.219). Other recognised or ascribed qualities given to, or claimed by, professions include technical proficiency (Evetts, 2011, p. 414; Wendel, 2000, p.563), authority and legitimacy (Evetts, 2011, p.414), and commanding the trust of those outside of the profession (Evetts, 2003, p.400).

The data indicates that while there are some of the above elements of a profession evident, these are not yet embedded or organised, and the professionalisation agenda, whilst present, is at a nascent stage. There is widespread recognition amongst participants that the work requires professionalism in terms of technical competence and that application of skill and judgement is necessary within the work and to enable intelligence sharing (CS/11, RI/11, RI/20).

> RI/20: "I think we underestimate the skill involved in intelligence sharing and intelligence handling. It's not recognised, we think it's data, and we think a couple of rules around that'll be fine. I think it's much more complex, and it involves professional people making professional decisions."

As such, and with the recognition that there is a lack of competence displayed by some parties (CS/11, CS/21, RI/13), there is the acknowledged need for people performing intelligence work, and sharing intelligence with others, to have the requisite skills and knowledge to do the job (RI/12, RI/22). As such, there is a call for both professional standards and recognition in some quarters, and indication of a shared professional identity amongst practitioners (Evetts, 2006a, p.518; Evetts, 2006b, p.134, Evetts, 2013, p.780).

There is undoubtedly a knowledge base, although it is clear that, whilst some standards are in place – especially applicable to the law enforcement sector – these are not yet codified and do not apply to all intelligence, counter fraud or IP crime practitioners working with, or sharing, information and intelligence. However, the standards to which law enforcement bodies operate were seen to be widely accepted by organisations in other sectors as best practice, and were adopted by FACT and by many other participants' organisations as such. These include the NIM as the business model (CS/22), MOPI as the general code of practice for information sharing (CS/18, RI/20, RI/21) and widespread use of the 5x5x5 grading system (CS/17, RI/03, RI/04, RI/06, RI/07, RI/14, RI/17B, RI/20, RI/22). However, as this is not legally required, not all organisations use them. Whilst FACT and several other participants stated that they adopt these standards in order to make it easier to share with law enforcement, some interviewees from law enforcement agencies stated that they did not necessarily expect or require this (RI/09, RI/11, RI/22). RI/14, from the retail banking sector, stated that he used the 5x5x5 information report when dealing with law enforcement, but not when dealing with other banks as they might not necessarily understand it. But there was a call for common standards, not just in intelligence handling and sharing, but also in data quality (RI/08) as trust in the quality and reliability of the data shared by partners is essential (RI/04, RI/06, RI/14, RI/18). In the anti-fraud arena too, there is no framework of best practice in the private sector (Brooks, Button & Frimpong, 2009, p.494), and only piecemeal adoption of public sector standards and processes.

There is no recognised professional institution for anti-fraud, IP crime or intelligence professionals that fulfils the functions of such an institute denoted in the literature on professionalism. RI/01 gave an impassioned argument in favour of one for counter fraud practitioners, arguing that a chartered institution would have continuous government monitoring of its rules, and should have the power to set and enforce standards and remove the accreditations of those that contravened rules in respect of intelligence sharing, allowing fraud specialists to be held accountable for inadequate information sharing practice. He was strongly in favour of properly trained and qualified investigators being given the power to share intelligence and to be held accountable for failures in process.

For intelligence professionals, there are some early movements towards professionalisation. Although there is no primary institutional body, the College of Policing has launched an Intelligence Professionalisation Programme [IPP] with the

intention of introducing accreditation and continuous professional development requirements (RI/13), although this will apply primarily to law enforcement practitioners. Furthermore, the college has announced its intention to seek chartered status (College of Policing, 2015a). Running in parallel to the IPP is an initiative from a NIM working group led by RI/13 encouraging universities to develop Master's programmes in intelligence handling. At the time of interview, RI/13 confirmed that three universities were due to launch such courses, which would be available to both law enforcement and civilian students, with talks underway with other universities. Additionally, the Counter Fraud Professional Accreditation Board, hosted by the University of Portsmouth, issues two accredited qualifications for intelligence professionals, at Technician and Specialist levels (University of Portsmouth, n.d.). This is a positive step with respect to the drive towards professionalisation, but the courses must reflect the requirement of providing not only qualifications to students in these subjects but also the competencies required in the workplace (Pavlin, Svetlik & Evetts, 2010, p.99). There is a market for such qualifications; both RI/19A and RI/19B expressed support for more qualifications in intelligence and fraud.

> RI/19A: "For me, there has been a massive industry push on people having CII accreditation but within that accreditation there is very limited fraud, there's very limited intelligence. […] So I think if the industry's concerned, intel sharing would be better if everybody was actually educated."

Other accreditations may also be pursued by organisations and information sharing schemes to demonstrate professionalism and the standards to which they adhere. At the time of interview, RI/03 stated that the intelligence sharing scheme that he represented was pursuing accreditation under the ISO27001 information security standard.

Without professional institutions in place, other key aspects of professionalisation are not present or not organised and controlled in the way of traditional professions. There is a knowledge and research base, and there are journals devoted to the intelligence and fraud fields, but these are not institutionally driven. Nor is there the formal control of access to the knowledge base centred around an institution, although alternative mechanisms for restriction to the knowledge and skills are there, such as restriction for some training courses to law enforcement staff, as well as controls imposed by vetting procedures ranging from Disclosure and Barring Service checks on criminal history to formal Security Clearance procedures (RI/12, RI/19).

Summary

Ensuring that people dealing with, and sharing, economic crime-related information and intelligence have the requisite knowledge, skills and competence to handle and exchange this data appropriately and legally is a matter of considerable concern to the stakeholders involved and to participants of the study. Without mutual confidence in the ability of practitioners on both sides of the information sharing relationship, collaboration will not happen, or will be limited in extent. As such, the role of training and education is an invaluable and important function in the operations of many organisations that successfully engage in information sharing. Equally, there was substantial evidence of many organisations adopting the default intelligence handling and sharing framework and standards used within law enforcement, despite there being no legal requirement for non-law enforcement agencies to do so. In the absence of other national standards, however, the benefits of their doing so are clear. In recognition of these factors, and the skills involved in handling and sharing intelligence, there appears to be a growing identification amongst practitioners that they are exercising professional judgement and skills, and that both anti-fraud work and intelligence work should be recognised as being professional in nature. While there are some indications of a professionalisation movement, this is clearly in its very early stages, and there was no evidence arising from the data of how such a professionalisation movement in both anti-fraud work and intelligence work may develop or harmonise across both functions, despite the overlap between the domains.

The findings outlined in this chapter, along with the three previous chapters, will be discussed further in Chapter Eight which will consider the findings together and how they reflect on the practices and structures that lead to effective inter-organisational intelligence sharing.

Chapter Eight

Discussion

Introduction

The previous four chapters set out the findings from the analysis of the data collected during the study, across four broad thematic areas. This chapter brings these findings together for further discussion of some of the most significant matters arising from the enquiry. It commences with a discussion of the primary challenges and barriers to information sharing identified during the study. This is followed by a review of the legislative framework, the issue of standards for intelligence sharing and strategies for managing collaborative relationships identified within the data. After this, some of the underlying models for information sharing relationships, as described by the participants are examined, followed by further discussion of the issue of professionalisation.

Barriers to Information and Intelligence Sharing

It is not possible to take a simplistic view as to whether or not most organisations within the UK are effective at sharing information or intelligence with others for the purposes of preventing, detecting, investigating or taking enforcement action against economic crime. Neither can such judgements confidently be made with respect to particular sectors or most industries, although there was a general consensus that the financial services industry was better than most. There is insufficient information published to ascertain how many organisations, and across which industries, are involved in this type of collaboration, or are trying to be. It is well documented, however, that information and intelligence sharing is an important, and potentially transformative, tool in the fight against fraud and IP crime (Doig & Levi, 2009, p.205; Fraud Review Team, 2006b, p.94). A more nuanced view must be taken with respect to how well organisations are at collaborating in this respect due to the complexity and sensitivity of the issues involved, and as a balance must be maintained between the sharing of personal data to combat crime and the need to protect privacy (Fraud Review Team, 2006b, p.93; ICO, 2007, p.4).

To this end, however, remain a number of barriers and challenges to information sharing that arise from the need to achieve this balance and which are ancillary to it. Unsurprisingly, many organisations have historically struggled and continue to do so.

The perceptions of research participants were varied, although it was generally recognised that organisations found information sharing to be problematic and not as simple as it could, and perhaps should, be. Furthermore, there was a great deal of inconsistency reported. Cross-sector sharing between public and private sectors was generally perceived to be poor, despite numerous calls for improvements and government initiatives to stimulate this over many years, both before and after the Fraud Review of 2006. Additionally, there was a perception of continuing problems in sharing between public sector bodies, despite this sector being host to many strategies to promote collaboration and – perhaps in some cases because of – having a multitude of legislative gateways intended to enable sharing. The central and long-standing perception has been the tendency for public sector organisations to expect private sector companies to supply them with information and intelligence but to share nothing back; this view was expressed by participants representing both private and public sector organisations. This supports findings from reviews of the efficacy of the legislative channel allowing public sector organisations to share information with designated SAFOs, in which failures by public sector bodies to understand and use the channel were recognised (ICO, 2015a, p.15; NFA, 2010a, pp.14-17), a problem that still persists. Consequently, there remains a reluctance in some private sector organisations, whether they are SAFOs or not, to share with the public sector due to the belief that they will receive nothing back.

This notwithstanding, there were also some optimistic messages from the research. There was acknowledgement that the situation was improving and recognition – again from those representing both public and private sector organisations – that there was more government support for collaboration, with participants from FACT, law enforcement and the private sector citing the 'dare to share' mantra. However, the evident problems that remain in cross-sector information sharing suggest that there is still much to be done to turn such rhetoric into effective and widespread collaboration.

In terms of the primary barriers to information sharing discussed by participants as being current at the time of data collection, a number of key issues remain as long-standing and ongoing challenges. Each of the factors cited most commonly by the participants as being major impediments to intelligence sharing were issues that have been previously documented in the literature. This is testament to the enduring nature of these problems and evidence of the failure of both policy and professional practice to resolve these despite repeated calls and commitments to improving and enabling

intelligence sharing at professional and governmental levels. Furthermore, as many of the problems previously identified within the literature did not necessarily relate to the anti-fraud context, although many did relate to collaborations within the criminal justice arena, it indicates that these issues will likely be enduring in other areas as well, some of which may not have enjoyed the level of political will towards improving intelligence sharing that the anti-fraud field has seen. This is of concern, but further exploration of it remains beyond the scope of this work. As was illustrated in Figure 4.1 in Chapter Four, the issues most commonly cited by participants as obstacles to information sharing were those of data quality, cultural reticence to share, the tendency for a one-way flow of information, incompatibility between systems, cross-jurisdictional problems and the volume of data to be transmitted, processed and stored. Each of these has been previously discussed in the literature (see Figure 2.1), although with respect to the issue of volume of information, the concern raised by participants was focussed on the volume of electronic data due to the information rich world in which organisations currently operate rather than the volume of data stored in non-digital form as identified within the medical emergency information sharing scheme discussed by Schooley and Horan (2007, p.771).

Some additional factors discussed with participants, however, were found to be more pronounced within the anti-fraud field than in the literature concerning information sharing in other contexts, even in other areas of criminal justice. Legislative problems, especially those relating to the DPA, were a particularly dominant theme in the data whereas, whilst legal and political issues had been identified within the literature, no single such legislative matter appeared to stand out to such a profound extent in other intelligence sharing settings. While the legislative framework will be discussed in the next section, the problems of hiding behind the DPA, lack of understanding of legislative provisions and fear of reprisals from the Information Commissioner were central themes in the interview data. Other than the grey literature relating specifically to anti-fraud intelligence sharing, these were not significant challenges found in the wider information sharing literature. Matters of competence in intelligence handling and sharing also form a central challenge in sharing data in the anti-fraud and IP crime contexts, and related issues of lack of trust in partners and deficiencies in training of practitioners have been identified in the literature (Figure 2.1). However, this may again be more pronounced in the anti-fraud field due to the large number of non-law enforcement actors involved in preventing and investigating these types of crime in both public and private sectors (Albrecht & Albrecht, 2004, p.15; Button, 2011, pp.251-252; Button & Gee, 2013, p.52; Smith et

al, 2011, pp.70-72). Accordingly, the levels of experience and competence of these will vary widely (Comer, 2003, p.225). The significance of these issues helps to explain the emphasis placed on the training of practitioners – both within their own organisations and, often, supplied to other organisations by those involved in intelligence sharing – identified in the research data.

Technological issues, relating primarily to matters such as system incompatibility, data quality (including inconsistencies in the format of data stored by different organisations) and the volume of electronic data are certainly still relevant. However, whilst these are challenges that must be faced by those processing and sharing intelligence for anti-economic crime purposes, solutions and fixes are readily available, from the agreement of data schema between partners to investment in bigger servers and technologies that can resolve these problems. So whilst these challenges are still extant, and they appear regularly in the literature, especially that of a decade or so ago (e.g. Bellamy et al, 2005, p.397; Levi & Wall, 2004, p.215), these can be resolved with sufficient investment and so may perhaps be considered to be primarily cost and resource issues in essence. The evidence from RI/20 and RI/21, from a government agency that had changed its intelligence system to be compatible with that of a key partner, Trading Standards, shows that these challenges can be overcome with sufficient commitment.

Cultural issues, such as the reluctance or refusal to share by people or organisations, remain enduring themes both in the literature and the research data. However, changing organisational culture can be a difficult, and often long-term, process. Organisational culture may be considered to be the shared values and beliefs that are collectively taken for granted and seen as non-negotiable from the basis of their historical success (Schein, 1996, p. 236; Schein, 2009, p.26). Corfield and Paton (2016, p.91) observe that, while culture may be resistant to change, organisations must be able to adapt themselves to face new realities in the current environment. Alvesson and Sveningsson (2008, p.40) suggest that there are three main positions on the management of organisational culture:

- that with the application of resources and skills, senior management may adapt culture
- that senior management may adapt culture, but it is difficult to achieve
- that culture is not controllable and, by implication, change may not be actively directed.

The challenge of changing culture is, therefore, well recognised. Schein (2009, p.21) defines three levels of culture:

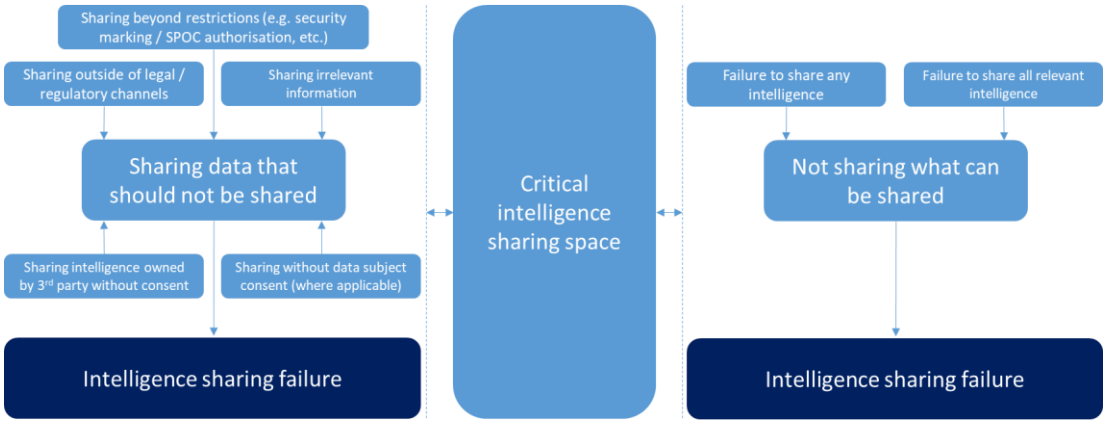
- artifacts: visible corporate structures and processes
- espoused values: organisational strategies, goals and philosophies
- underlying assumptions: tacitly accepted norms which are the source of values and action.

It is this third layer that must be changed to truly overcome some of the key challenges faced in intelligence sharing, although this change may be directed and supported by change in the other two. This layer is the most difficult in which to enact change due to those assumptions being formed and held subconsciously; employees may not be aware of deficiencies in the existing cultural norm (Limwichitr & Broady-Preston, 2015, p.484). However, is possible to achieve change in information sharing behaviour, as in other areas. Heller (2002, p.51) argues that, while most change programmes seek to change culture first, followed by behaviour, the real object is to change people's actions first, and cultural change will follow. Anti-fraud collaborations may be considered as security networks, described by Whelan (2015, p.2) as relationships between multiple entities within the security field, and in which culture is one of the most significant properties. Whelan goes on to observe that cultural change occurs as agencies work together (2015, p.18), whilst Powell (1990, p.324) states that the sharing of information between partners itself can lead to the building of common values.

Whelan states that there remains a significant gap in understanding of how security networks achieve cultural change (2015, p.8). The findings from this research indicate that, within the anti-fraud and IP crime fields at least, the commitment of time and resources to programmes of education and training, not only of internal staff but of staff and senior managers within partner agencies and prospective partners, is an important strategy employed to achieve this end. Given the challenges faced in this area, such training tends to focus on primary issues such as the nature of the problem, the legal framework for sharing and key aspects of intelligence handling in line with standards such as the NIM and MOPI. The active involvement and support of senior officers of the organisations involved is also an important factor in effecting cultural change pertaining to information sharing.

One final challenge relates to the issue of intelligence sharing failure. This is normally framed in terms of the failure to share intelligence, but in the discussions with FACT, supported by data from other participants, it is clear that there are two main angles of intelligence sharing failure: the failure to share information, and the sharing of data that should not be disseminated (Figure 8.1). Both present significant problems in respect of effective collaboration and the maintenance of trust, while the area between these two positions is the critical intelligence sharing space in which sharing is both appropriate and necessary.

Figure 8.1: Intelligence sharing failure and the critical intelligence sharing space



Legislative Framework

The research has provided data on the legislative framework available to organisations in the private and public sectors in respect of information sharing, and of the channels that are utilised. It has provided further insight into some of the complexities and challenges with respect to this legislative infrastructure relating to intelligence sharing for anti-fraud and IP crime purposes.

The findings focussed on three main topics, these being: the DPA and the exemption within s.29(3) relating to the disclosure of personal information for the prevention and detection of crime or the apprehension and prosecution of offenders; the gateway under s.68 of the SCA allowing public sector bodies to share information with SAFOs; and the legal gateways available to government departments for sharing information relating to fraud and financial crime. Overall, the message echoed that which has been previously expressed in the literature; the general legal framework exists to enable organisations to share information and intelligence, but the law in its current form is poorly understood and regularly misinterpreted and misapplied.

The SCA provisions in respect of SAFOs is not being adequately utilised by public sector bodies to share with those private sector bodies so designated. The evidence suggests that many public sector bodies remain unaware of the provision, do not understand it, or are unwilling to use it. As such, this channel does not adequately fulfil its purpose of enabling cross-sector sharing. Even when it does work, there remain so few bodies recognised as SAFOs that the provision remains extremely restrictive in its scope and potential. This suggests that there has been limited progress since this channel was first established, despite reviews of the efficacy of the provision by the NFA (2010) and the ICO (2015a) highlighting these problems. Some participants in the research represented SAFOs; they reported that, with a few exceptions and some limited progress, that the channel was not working as intended or hoped.

Likewise, the situation with respect to legal gateways for government departments to share information for anti-fraud purposes gives little confidence that government policy is travelling in the right direction. The landscape of these provisions is complex and confusing, with myriad specific gateways in place and little clarity over which take precedence (Law Commission, 2014, p.26). These are generally very restrictive in terms of scope and applicability, and result in a fragmented and misunderstood framework. This continuing situation was a concern raised by several participants, who commented on the over-complexity of the provisions and the lack of flexibility allowed when the government continues to create – often at the behest of individual departments such as the DWP – gateways designed to allow limited sharing in response to specific criminal activity in precisely defined circumstances. Where criminals continuously adapt their techniques and targets, this direction of travel is not only misguided but counterproductive, and is moving in the opposite direction to the simplification of primary legislation with respect to the core offences of fraud and bribery. There was serious dissatisfaction expressed by participants at the current approach, and call for simplification and reform towards the creation of clear, broad channels to improve information sharing between and by government bodies. However, as noted in Chapter One, the government appears to be continuing along the path of creating new specific gateways such as that created in the Digital Economy Act 2017.

The exemption on disclosure of information in s.29(3) of the DPA was shown to be a major issue for those sharing information and intelligence for economic crime purposes. Participants saw the scope of the provision as providing a clear and

sufficient opportunity to allow relevant sharing between partner agencies, and the ability to do so legally. As such, this exemption forms the legal basis upon which most participating organisations, within both public and private sectors, based their information sharing relationships and arrangements. This was also detailed in the MOUs, contracts and service level agreements used by many participants, and was central to the agreements and approach used by FACT. Where participants didn't have formalised agreements in place, s.29(3) requests were often still used to request information from other parties on an ad-hoc basis.

However, despite this reliance and general consensus that it provided a workable legal foundation for exchange, the data also confirmed that the DPA continues to provide significant obstacles in respect of information sharing. Substantial concerns were voiced by participants across both phases of the data collection. These focussed on serious issues such as lack of clarity in the legislation, serial and widespread misunderstanding and misinterpretation of it, and using the DPA as a shield by which to avoid sharing information rather than utilising the exemption as a means to enable it. Additional concerns related to fear of the consequences of breaching the Act and enforcement action from the ICO if it was used incorrectly. These problems seem not to be constrained to the private sector, but were reported to affect public sector bodies and law enforcement agencies as well, and seriously impede information sharing within and across sectors. These problems have been well documented within the grey literature and recognised as challenges for a long time, having been noted as serious issues within the Fraud Review (2006b, p.100). Similar problems have been noted with respect to the DPA for other criminal justice failings beyond the fraud and IP crime arena, such as in the Bichard Report (2004) into the Soham murders. It is disappointing that little progress appears to have been made in this area, despite widespread recognition of the problem and the publication of guidance and codes of practice intended to provide clarification. This failure means that, despite confidence in the adequacy of the provisions, the application of the legislation remains dysfunctional and impedes information and intelligence sharing. Additional guidance has been issued by the ICO (2015b) since the data collection was completed; while the impact of this cannot be determined from the research data, it seems reasonable to conclude that this alone will be insufficient to tackle the deep seated dysfunctionality of the DPA in respect of information sharing.

Education and awareness, and setting out the legislative framework within MOUs and similar documents, remain the key strategies employed by organisations to overcome

these problems, but the prospects for success of these approaches will be constrained without government intervention and simplification or clarification of the law. Furthermore, while this provision remains the primary general basis for sharing, it is further constrained by being an optional, rather than mandatory or recommended, conduit, and qualifying requests under s.29(3) may be refused by the recipient. This provides potential contradiction and conflict with the finding that there is greater general impetus to share, and government initiatives to encourage it, including the "dare to share" mantra.

However, clarity on data protection law appears to be an unlikely prospect for some years to come. On 24 May 2016, the EU General Data Protection Regulation [GDPR] came into force, with the objective of harmonising data protection rules across all EU member states (Linder, 2016, p.108). Despite the UK's referendum vote to leave the EU [Brexit] in June 2016, the GDPR will apply in the UK in May 2018 when the Regulation takes effect across EU member states as the UK will not have left the EU by this date (ICO, 2016, p.3); thus it will have force of law in the UK, replacing the DPA. The impact of the GDPR on information sharing is beyond the scope of this thesis, as it had not been published at the time of data collection, although most participants, including FACT, confirmed during interviews that they were closely monitoring developments in this area. However, the change in legislation will undoubtedly introduce uncertainty and change in respect of data sharing, and the full implications and determination of rights and powers under the GDPR will be subject to debate and legal tests for many years to come (Calder, 2016, p.1). Given the lack of clarity evident with respect to the DPA, the changes with the GDPR will ensure uncertainty for the foreseeable future. Furthermore, it remains to be seen whether the GDPR will remain in full force, or if it will itself be changed and replaced, following the UK's eventual exit from the EU.

Standards

While there is a provisionally adequate, albeit flawed and dysfunctional, legislative framework in place that can enable information sharing, there is no such established set of national standards that govern the practice of information sharing or intelligence handling across all sectors. There are standards in the law enforcement arena, including the NIM, MOPI and the 5x5x5 grading system (superseded by the 3x5x2 model after the data collection had taken place). These have collectively become the benchmark, and the default standards that many information sharing models have

adopted, despite being designed primarily for use in the law enforcement environment.

FACT has based its operating model as an intelligence-led organisation around the central tenets of the NIM business model. This can be seen in its adoption of key structures and processes prescribed by NIM: from maintenance of a Control Strategy setting out its strategic direction; the running of Tasking and Coordination meetings; the recording and dissemination of intelligence on information reports using the 5x5x5 grading process; and its production of core intelligence products described in NIM, including its Strategic Assessment, Target Profiles and Problem Profiles (ACPO Centrex, 2005). This is fundamental to FACT's approach both to its operational model and its strategy for collaboration with partner agencies as it means that it produces intelligence products that its key partners – law enforcement agencies – recognise, understand and are confident to act upon.

Many other participants in the research also advised how their organisations adopted parts of the NIM process and outputs, grade incoming or outgoing intelligence according to the 5x5x5 model and adhere to MOPI guidelines for similar reasons. In the absence of a formal national standard across all sectors, the law enforcement framework has become the de facto standard to which many, although not all, organisations and intelligence sharing schemes align.

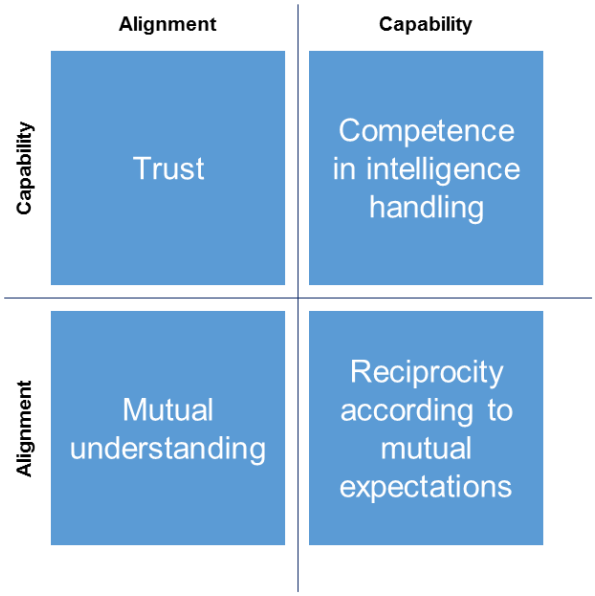
However, just as FACT follows the spirit of the model, but does not rigidly apply every aspect of it (CS/18), neither do the other private sector organisations that adopt, or adapt, parts of the NIM business model. They can, and do, pick and choose which elements to apply in accordance with their own procedures and needs. This is inherently sensible, as the NIM was designed to apply to a law enforcement environment, supporting a diverse range of policing issues and operating at three levels: local; cross-border and organised crime (NCIS, 2000, p.8). Much of the model may not be relevant or appropriate to non-law enforcement bodies and businesses. Herein also lies the danger. Where organisations will pick and choose elements of a default adopted model in the absence of national standards, and may interpret and apply them according to their own needs and criteria, such practice risks devaluing the model as a whole. Whereas FACT demonstrably goes to considerable lengths to maintain high standards and produce high quality intelligence products, not all organisations may be so rigid. This risks undermining trust in the whole system and making professed adherence to the NIM, or other standards, meaningless outside of

the law enforcement arena. Accordingly, this could undermine this key strategy of those organisations that do use the NIM appropriately to enable intelligence sharing and maintain trust with partners. This is one of the many problems and risks that arises not only from the lack of national standards for intelligence handling and sharing, but the lack of a national intelligence strategy that takes all sectors into account and the absence of a central body to maintain oversight of this.

Relationship Management

The foundation of effective information sharing is having strong relationships with partners. Analysis of the data collected suggested that there were four key, and interlinked, aspects of such a relationship: trust; competence, mutual understanding and reciprocity. These elements are inter-related in terms of how they reflect organisational capability of handling and disseminating information and intelligence, and of how collaborating partners' goals and needs for the relationship have been aligned (Figure 8.2). These issues had been variously identified in the literature, with barriers of lack of trust identified by, amongst others, Canestraro et al (2009) and Schooley and Horan (2007), one-way flow of information by Zheng et al (2008) and lack of understanding by Bharosa et al (2010). Competence in intelligence handling has been less directly covered, although competence issues have been both inferred and discussed in respect of discrete matters such as data privacy (Boba et al, 2009). The data confirms that all of these factors are essential, although reciprocity may be subject to mutual acceptance of more information flowing in one direction than the other if this serves the interests of both parties. Given the range of organisations across all sectors to which counter fraud work pertains, competence is perhaps a more significant factor in anti-fraud intelligence sharing than other criminal justice arenas for reasons of scale alone.

Figure 8.2: Prime attributes of effective information-sharing relationships



There are a number of key strategies employed by participating organisations that address these issues. Training and education of internal staff and, perhaps crucially, training of partners' staff (and members of intelligence sharing schemes) is central to their success. Adherence to – and training to – the default standards (e.g. NIM) is an important part of this. The involvement of senior officers is also valuable, especially in establishing relationships and developing understanding, as well as from the basis of having people involved who have the authority to make decisions on behalf of their organisations. Likewise, many participants reported that the use of SPOCs, both as contact points and gatekeepers who are responsible for maintaining agreed standards, are important. These findings reinforce the previous identification of these within the literature as enablers to sharing. The role of MOUs and contracts, also acknowledged within the literature, was an important element within anti-fraud information sharing. These were extensively used by FACT and other participants in formalising relationships. MOUs set out the agreed processes and standards and help to cement trust and understanding between parties. This can be reinforced by the agreement and conduct of audit and compliance processes (also an important element of the mechanisms described by many participants).

Trust may also be influenced by underlying motivation. While there are services for the sharing of intelligence that are profit-orientated, it is notable that FACT and all of the industry-based schemes that took part in the research were non-profit making entities, with boards comprised of representatives of member firms. This may not be

an essential factor, but it may help to strengthen trust amongst those participating in the schemes as there is no secondary motive.

The issue of reciprocity is an important one, as the one-way flow of information can critically undermine a relationship where both parties are expectant of receiving information in return for that which is given. Public sector bodies received significant criticism from participants on this point. However, the levels of information that must be shared in each direction will be different for each relationship. Many of the industry-based information sharing schemes specifically audit members' provision of information. But this is not necessarily critical in every information sharing relationship. FACT officers generally stated that they were content to act primarily as providers of information to their partners (especially law enforcement) as this fulfilled FACT's needs, which was to get these agencies to take action. RI/21 was similarly inclined. The crucial element of success then, is not necessarily that both parties will have equal flows of information incoming and outgoing, but agreeing expectations. If both partners are content with a majority, or even all, information and intelligence to be flowing in one direction, and expect this to be the case in operation, the relationship can work well on that basis. It is where expectations are not fulfilled in reality that problems will arise; this further underlines the importance of mutual understanding.

Two concerning issues arise from the data in respect of relationship management. Firstly, many information sharing relationships rely on the private networks and personal contacts of the staff working in anti-crime functions. Often these will be based on historical relationships between, or affinities held by, ex-law enforcement officers. This is primarily due to the similar experiences and understanding that such a shared background brings, and an initial trust in the standards to which intelligence will be processed and graded. As such, this can be a practical substitute in lieu of recognised national standards and accreditation in anti-fraud and intelligence handling work. However, it does serve to exclude practitioners and organisations without access to this relevant experience, and may impede their abilities to build and engage in productive information sharing relationships. Secondly, there continues to be reliance on informal and off-the-record sharing, some of which may technically be illegal or, at least, outside the spirit of the legislation. This is often followed up by a formal s.29(3) request if it is confirmed that the intelligence is there and is relevant. Such activity will invariably fall on a spectrum, ranging from a preliminary informal steer through to non-documented provision of sensitive intelligence and personal data; at one end this may constitute illegal behaviour and abuse of process. Again,

the lack of clear national standards and central oversight could be a factor in this activity.

Models of Information Sharing

During the interviews, several different models of data sharing were discussed by participants, either in respect of how the organisations that they represented structured their information sharing relationships or described from their previous experiences. While these models were subject to varying amounts of complexity and detail in operation, the underlying structures of these have been represented in Figures 8.3, 8.4 and 8.5 below.

Figure 8.3: One-to-one information sharing (three variants)

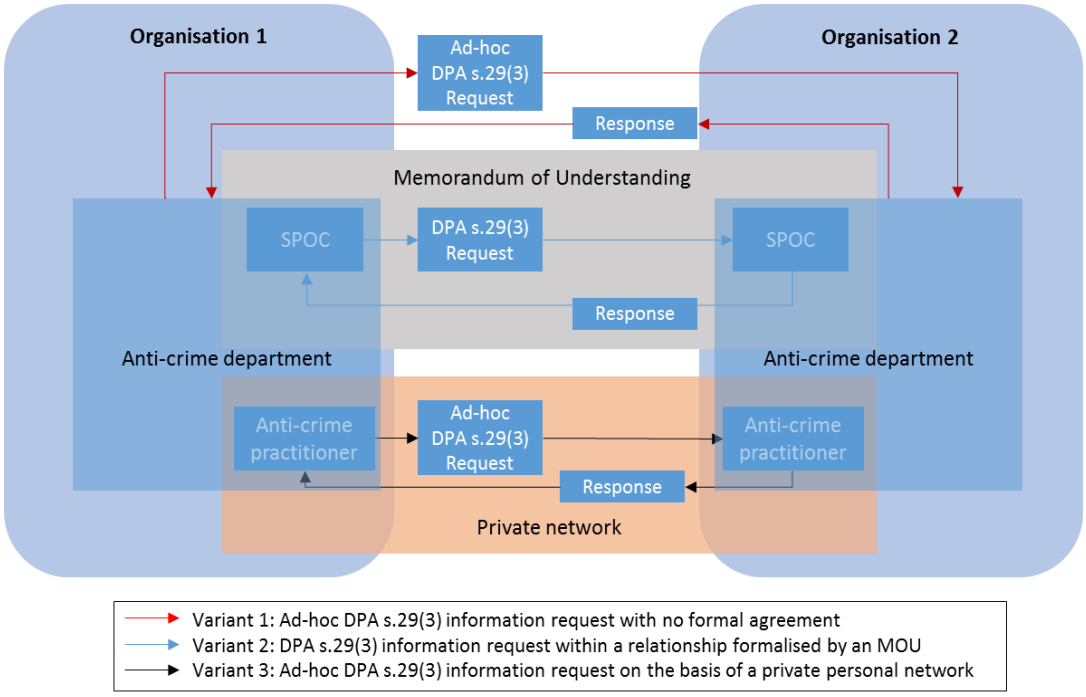


Figure 8.3 summarises three commonly used variants, described by participants, of models for inter-organisational information sharing based on the use of the DPA s.29(3) exemption.

Variant 1 illustrates an informal information sharing relationship, whereby an officer in an anti-crime department of Organisation 1 makes an ad-hoc request for information under s.29(3), relating to an incident under investigation, to a similar department within Organisation 2. Providing that the request satisfies the requirements of s.29(3), Organisation 2 may decide whether or not it chooses to provide the information requested. Organisation 1 has little basis for determining

whether or not Organisation 2 is likely to be inclined to cooperate. This is the default model under which most organisations will operate, unless they have information sharing agreements in place with other parties.

Under Variant 2, the information request is made by Organisation 1 to Organisation 2 using the same underlying legal basis for the appeal. However, in this model, the two organisations have an MOU in place that sets out the basis of their information sharing relationship, and under which each organisation has nominated SPOCs to act as gatekeepers for this purpose. The SPOC for Organisation 1 issues the s.29(3) request to the SPOC for Organisation 2 who will make the decision as to whether to accede to the request if it is determined to meet the s.29(3) criteria. While Organisation 2 is still not obliged to cooperate under this model, even if the sharing would be legal under the DPA, it is far more likely to be amenable to the request as there is a formal relationship in place, the protocols for collaboration and exchange of information and intelligence are agreed and documented, and there are established points of contact through which requests made under the MOU are made. This is the optimal of the three variants, and most likely to result in successful sharing of information, and is the essence of the model used by FACT, as well as other participants in the study.

Variant 3 describes an informal information sharing relationship between two organisations similar to that depicted in Variant 1. However, the s.29(3) request is made by an officer in Organisation 1 who has a contact in Organisation 2 on the basis of their private network, such as a shared history in law enforcement. The request operates in the same manner as that for Variant 1, but may be more favourably received and responded to by the recipient in Organisation 2 on the basis of their personal relationship. While this can be beneficial in the immediate circumstances of the information request illustrated in Figure 8.3, and can lead to successful sharing and collaboration, this model bears the risk of failure should either of the parties in the private network leave their positions in their respective organisations, in which the basis of the collaborative relationship and mutual understanding would be lost, and the two organisations would be left with the model illustrated in Variant 1.

Figure 8.4: Hub-and-spoke model (externally searchable database)

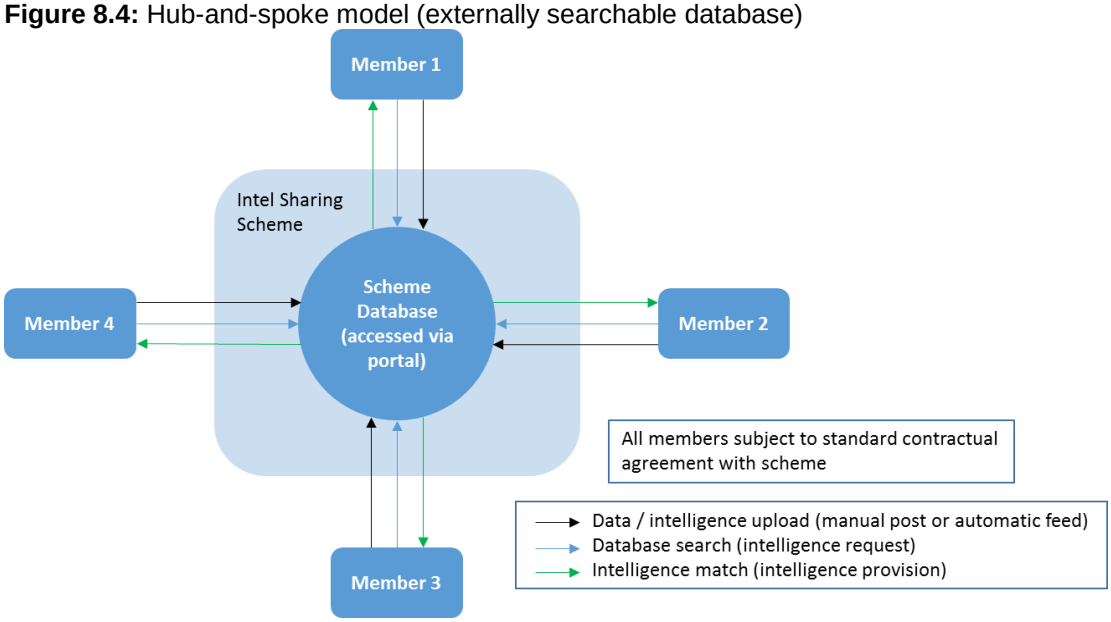


Figure 8.4 depicts the underlying model of information sharing used by several of the information sharing schemes that took part in the research, including those represented by RI/04 and RI/06. In this, scheme members agree to a standard agreement that documents the rules and responsibilities of the relationship, in a similar manner to an MOU but having a single agreement that applies to all members rather than individual terms for each organisation. Under the agreement, members of the scheme will upload appropriate anti-crime related information or intelligence that is organised and stored by the scheme in a central database. When members are seeking information, they will access the scheme's database via a secure portal, or other established means of access, and search for the information that they require. If information meeting the search criteria has been uploaded by another scheme member, this will be accessible by the member searching for it providing that the request and exchange meets the rules set by the scheme (and potentially subject to further restrictions on access to the information set by the provider). This is a model that can enable successful many-to-many information sharing.

Figure 8.5: Hub-and-spoke model (onward referral via central coordinator)

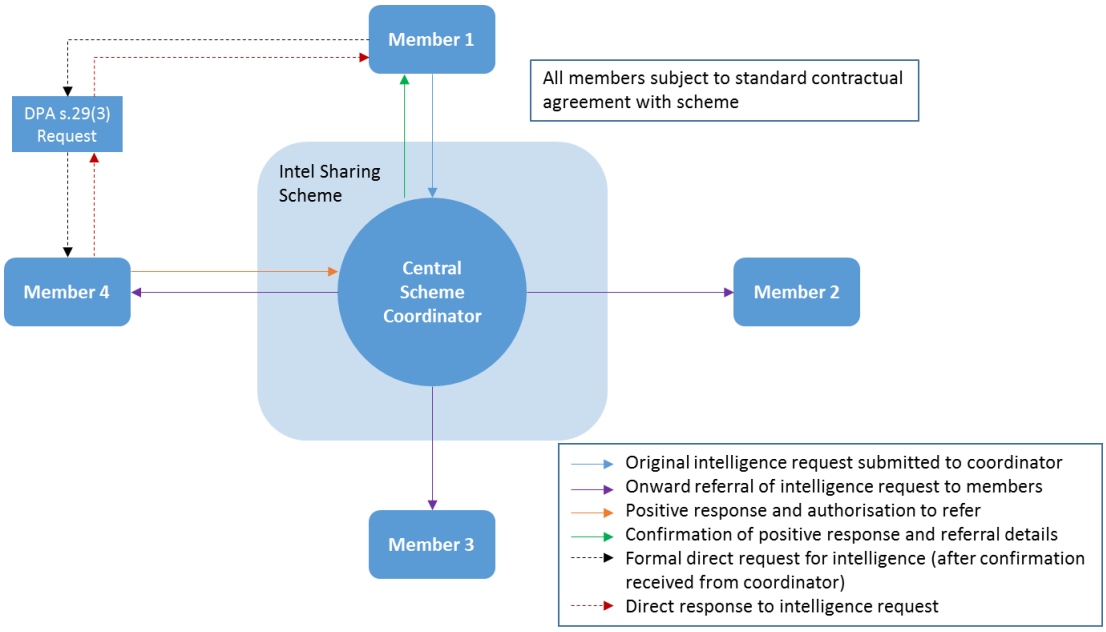


Figure 8.5 also illustrates a model used by information sharing schemes, and one that can be suitable to enable information and intelligence sharing between multiple parties. It shares similar characteristics to the model described in Figure 8.4 in that scheme members agree to a standard set of rules and responsibilities that govern the scheme. However, instead of information being uploaded and made available for access through a repository accessible to all members, the scheme relies instead on a central coordinator to facilitate intelligence sharing between members on a one-to-one basis (or a one-to-many basis if multiple members hold relevant intelligence). In this model, a scheme member will submit an intelligence request to the scheme coordinator. The coordinator, in turn, will push this request out to other members to seek confirmation of whether they might hold relevant intelligence that would satisfy the request. If another member does have this, and is willing to share it with the requestor, it will notify the coordinator, who in turn will notify the requestor and provide the contact details of the responding member. The requestor will then submit a formal information request, under DPA s.29(3), to the responding member, detailing the request in full. The responding member will then make a decision whether or not it is willing to provide the intelligence that it holds to the requestor in response to the formal request. This model provides the basis on which the schemes represented by RI/12 and RI/15 operate.

Call for Professionalisation

Given the range of challenges in sharing information and intelligence for anti-fraud and IP crime purposes, the number and diversity of organisations potentially involved and the factors involved in ensuring success, there is inevitably a call and need for greater professionalism in both intelligence handling and anti-economic crime work. This is driven by a mix of the complex legal environment, the sensitivities and skills required in the work, the lack of a national strategy, coordination or oversight and the daunting breadth and scale of the economic losses caused by fraud and IP crime. Practitioners recognise that they need training, accreditation, recognition and a body of standards to which to adhere, all of which were repeated themes in the research interviews in both phases of data collection.

Professionalism, and what constitutes a professional, can be viewed through several different lenses. It can be considered as a state-sanctioned recognition of the status and value of an occupation, and a privileged category that deliberately sets it a profession apart from other vocations (Edgley, Sharma & Anderson-Gough, 2016, pp.15-16). In the military intelligence context, importance is also placed on the concept of a profession being able to self-regulate and operate with limited external interference (Kreuzer, 2016, p.581), a logic that applies within other contexts with varying degrees of accuracy. As was discussed in Chapter Seven, there are many identifiable characteristics that have been used to define or describe the concept of a profession, including those of specialised education and training, professional institutions setting standards and applying control over access to a body of knowledge as well as the application of judgement and skill by the professional. This latter is perhaps especially resonant given the importance that interviewees gave to the issue of competence in handling and sharing information and intelligence both appropriately and legally. Professionalisation is the process to achieve such status and for the work of practitioners to demonstrate and uphold such standards. This was called for and otherwise discussed by many participants, most prominently and extensively by RI/13.

The data indicated that very early, tentative steps are being made in this direction within the intelligence field. This includes initiatives to establish higher education qualifications in intelligence handling and more professional training being developed, including the IPP by the College of Policing which has also announced that it will seek chartered status. In the absence of extant professional bodies, however, there was evidence from participants of organisations taking it into their own hands to improve

standards and skills through the provision of training to their own and other organisations' employees and members in order to provide them with the underlying skills and knowledge to handle and share information legally and effectively.

However, these are early steps, and will on their own have limited potential to extend to the wide range of practitioners across all sectors and industries involved in intelligence and anti-economic crime work. Without a co-ordinated intelligence strategy incorporating all sectors, and central oversight of this, the risk is that any moves toward professionalisation that do occur will be focussed solely in one sector, such as law enforcement or the public sector, to the exclusion of others. This could serve to improve intelligence handling and sharing within these areas, but could compound existing problems elsewhere and may further undermine cross-sector information sharing by reducing trust in the skills and standards employed by practitioners in excluded sectors. This would therefore strengthen the hand of criminals involved in fraud and IP crime for years to come.

The issue of professionalisation, the tentative steps towards it, and the recognised need for it was an underlying theme running throughout the study. Many of the key issues that emerged from the interviews across both phases of data collection are closely linked to it, either explicitly or implicitly. The importance of adhering to consistent standards in information and intelligence handling and sharing, the requisite emphasis on quality of data and outputs and the roles of trust and reputation in ensuring effective information sharing relationships were consistent themes, and inherent in the underlying conception of professions and professionalism. Likewise, in the current absence of broad, cross-sector standards for information and intelligence handling and sharing, efforts to attain and adhere to these can be seen in the adoption of the standards and practices in law enforcement and industry-wide standards (such as those in the insurance sector) point to this need and drive. Similarly, the resources expended on the training of participating organisation's own employees and those of partners, plus equivalent training provided by some of the information sharing schemes to their members, further demonstrates the recognition of the need to apply 'professional' judgement and skill, and the value of consistent and appropriate standards, processes and quality as well as legislative compliance in information sharing. Progressing the professionalisation process across all sectors would be a significant step in encouraging and enabling information and intelligence sharing within and across sectors in the UK.

Summary

Information and intelligence sharing in the anti-economic crime context remains subject to a complex array of challenges and barriers that reduce participation and prevent the benefits of collaboration from being more widely realised. While these challenges are not unique to the economic crime setting, they are amplified by the sheer number and range of actors with interests in this area. Furthermore they are exacerbated by a legal framework which, while for most parties does allow for appropriate information sharing, suffers from over-complexity, lack of clarity, widespread misinterpretation and uncertainty, the latter of which is likely to be compounded for years to come with the forthcoming introduction of the GDPR. While these problems are substantial, the data has shown that the devotion of resources to training and education of internal employees and those of partners is a key strategy to successfully collaborating in this legal environment. The adoption of, and alignment with, standards prevalent in law enforcement – in the absence of more widely applicable guidelines – is also a widespread strategy, although there are dangers inherent in the differences in how these may be interpreted by different parties, so this would benefit from coordination and oversight. There are a variety of structures and models employed to facilitate effective collaboration, and these can be utilised to enable bilateral or multilateral information sharing relationships. These frameworks can be bolstered further by a range of relationship management strategies to achieve the most effective outcomes for those involved.

The next chapter brings these themes together, and examines them against the research questions to set out the final conclusions of the study, as well as examining the contribution to knowledge that this enquiry has made.

Chapter Nine

Conclusions

Introduction

Following the presentation and discussion of the findings of the research in Chapters Four to Eight, this chapter sets out the key contribution made to knowledge of information and intelligence sharing in the economic crime context, and presents the overall conclusions of the study. These are presented with reference to the research questions raised in Chapter One.

Contribution to Knowledge

This research has contributed to knowledge of economic crime-related information sharing in several ways. It is the first time that a UK-based organisation in the IP crime arena has been examined by way of a case study into its operations with respect to intelligence handling and sharing, allowing greater understanding of the means by which it undertakes information sharing activities with partner agencies. The study has added to the body of knowledge on anti-crime information and intelligence sharing, and has substantively enhanced that with specific respect to organisations operating in the anti-fraud and IP crime fields. It has also added in a modest way to our understanding of intelligence failure within anti-economic crime information sharing by identifying inappropriate intelligence sharing as a type of intelligence failure. Finally, although it did not explicitly set out to do so, it has made a contribution to our understanding of how security networks achieve cultural change.

Any research of this nature will invariably raise new questions and leave other areas open for new and further exploration. There is considerable scope for further work to be undertaken in several topics relating to this subject area, including in the following directions:

- whether the general adoption of a non-mandatory set of standards, designed specifically for use by a particular sector, in lieu of a general standard for intelligence handling and dissemination, will result in that standard losing its value as a benchmark of reliability through inconsistent interpretation and application, and the extent to which this occurs

- the impact of legislative change, including the introduction of the GDPR and any further developments arising from Brexit, on information and intelligence sharing
- the process and development of the drive towards professionalisation in intelligence handling, the extent to which this occurs across all sectors, and the impact on any sectors or industries that are excluded from this process.

Conclusions

In order to conclude the study, it is worth briefly revisiting the questions set in Chapter One that framed the scope of the research.

What are the Contemporary Barriers and Challenges to Information Sharing?

As a general observation, the primary challenges to sharing information and intelligence to combat economic crime are broadly similar to those challenges in sharing data in other criminal justice fields. The main challenges cited by participants are summarised in Figure 9.1, organised into technical, organisational (non-cultural and cultural) and political classifications. The real challenge in respect of economic crime are that these issues affect a diverse range of organisations across all industries and sectors, rather than being the preserve of law enforcement agencies, and the practitioners that face and try to overcome them have equally diverse backgrounds and skills. These problems are compounded further by the lack of national standards which makes it difficult to establish benchmarks for quality and reliability against which trusted relationships could be forged. Furthermore, the legal framework is complex, misunderstood and, following the Brexit vote and the forthcoming introduction of the GDPR, subject to years of change and uncertainty ahead.

Figure 9.1: Economic crime information sharing barriers

What Strategies can be Deployed to Overcome these Challenges?

Organisations can overcome the challenges to information sharing. The focus should be on establishing trust and mutual understanding of processes and outcomes, and ensuring that the practitioners involved have the requisite skills and knowledge to handle and share intelligence competently. Key strategies employed, both by organisations in one-to-one data sharing relationships and by intelligence sharing schemes, emphasise aligning to best practice standards such as the NIM in the absence of mandatory requirements, formalising relationships and expectations through MOUs or contractual documents, and investing in training, education and awareness of both internal staff and those of the other party. These strategies can be readily adopted by other organisations given sufficient commitment and resource, and there is no reason why any organisation could not get to a position whereby it can successfully exchange information and intelligence with others to combat economic crime. Competence, quality, trust and reputation are key elements in building and maintaining collaborative relationships. Mutual understanding – including agreeing expectations in respect of the issue of the direction of data flow and levels of reciprocation by each party, and aligning this to the needs of all participants – is also essential if the relationship is to be productive, mutually beneficial and effective in the longer term.

How Can Professional Practice be Improved to Overcome the Challenges?

In order to extend successful information and intelligence sharing on a widespread basis across all industries and sectors, and between sectors, professional practice needs to be improved at three levels.

At the operational level, practitioners need to be competent at handling, storing and disseminating sensitive and personal information and intelligence. If they are to adhere to the default standards, they need to be competent in applying the requisite skills and judgement in line with best practice in a manner that is proportionate, responsible and within the legal framework, and consistently with those standards.

At the strategic level, organisations need to commit to intelligence sharing relationships if they aspire to having these. This requires allocation of appropriate resources and demonstrating senior level support to ensure that practitioners can receive adequate training, and have the necessary processes and systems to process and disseminate intelligence appropriately. This must be supported by a

culture – in either the organisation as a whole, or at least within the relevant departments – that supports information and intelligence sharing. Those responsible for building and maintaining the relationships for all parties need to be clear about the expectations of each party, and deliver on these.

At the government policy level, there is an urgent need for national standards to be set for intelligence handling and sharing, and for an intelligence strategy covering anti-crime intelligence that incorporates organisations operating outside of the public sector. The present situation, whereby private sector organisations align their approach to law enforcement standards is understandable in the absence of a mandated cross-sector standard, but may ultimately result in trust in these standards breaking down where organisations adopt parts of the NIM in a piecemeal way and interpret and apply it inconsistently. This risk was previously identified in policing, with MOPI introduced to promote uniformity of application (John and Maguire, 2007, p.207). There is, therefore, similar need for such a mechanism in respect of wider adoption of the NIM framework.

Support should also be given to the tentative professionalisation agenda that is emerging in both the intelligence and counter fraud fields; this will need government support and oversight to ensure that it applies across all sectors to the benefit of the economy as a whole. Finally, in an environment in which significant change can be expected over the coming years to the legal framework in which information and intelligence sharing must take place, the government must work to ensure that sufficient clarity and guidance is given as early as possible to allow organisations to work to a common understanding of the emerging legal requirements. The current legislation is excessively complex and commonly misunderstood. The necessary changes over the coming years will create further uncertainty but should be used as an opportunity to work towards creating a clear legal framework within which organisations across all sectors can share information competently and appropriately in order to effectively combat fraud, financial and IP crime.

Concluding Comments

Because of the range of organisations and practitioners involved, and the convoluted and opaque nature of the current legal framework, information and intelligence sharing in the anti-fraud and IP crime fields is a complex matter. The underlying aim is simple: to effect proportionate and appropriate sharing of information in a legal

manner between organisations to prevent, detect, investigate or pursue action against criminality. In practice, however, it is a difficult end to achieve.

This research has shown that some organisations do manage to do so effectively and appropriately, and that there are benefits to all parties that achieve this. Many of the strategies that they employ can be readily adopted and replicated – with the application of sufficient commitment and resource – by others.

However, elements of the strategies on which this success is built are based on fragile and uneven foundations. These may both undermine the prospects for ongoing intelligence sharing and exclude other organisations from realising the benefit of this valuable tool for mitigating crime risks. There remains significant reliance on informal networks and the relationships between practitioners who are ex-police officers, described by one participant as an 'old boy's network'; a potentially ironic situation given that many intelligence analysts within police forces are civilians (John and Maguire, 2007, p.203). While this can work for those organisations with the relevant contacts in place, it does imply that other organisations may be at a disadvantage. The reason for this situation is readily apparent: the mutual trust in the application of intelligence handling standards understood by current and former law enforcement personnel. The surest way to overcome this hurdle would be for the introduction of an integrated national strategy, the setting of national standards that apply across all sectors and that are translatable between them, and the introduction of training and accreditation processes that can be accessed by practitioners in all sectors. This is a lofty aspiration, but the potential benefits that could be realised across the entire economy by enabling organisations to take advantage of intelligence sharing to combat fraud and IP crime would make the investment and commitment worthwhile.

References

6, P., Bellamy, C., Raab, C., Warren, A. & Heeney, C. (2006). Institutional shaping of interagency working: managing tensions between collaborative working and client confidentiality. *Journal of Public Administration Research and Theory, 17*(3), 405-434. doi: 10.1093/jopart/mul018

6, P., Raab, C. & Bellamy, C. (2005). Joined-up government and privacy in the United Kingdom: managing tensions between data protection and social policy. Part I. *Public Administration, 83*(1), 111-133. doi: 10.1111/j.0033-3298.2005.00440.x

ACPO Centrex. (2005). *Guidance on the National Intelligence Model*. Retrieved from https://whereismydata.files.wordpress.com/2009/01/national-intelligence-model-20051.pdf

ACPO Centrex. (2007). *Practice advice: introduction to intelligence-led policing*. Retrieved from http://www.fraw.org.uk/library/direct_action/acpo_2007.pdf

Aisopos, F., Tserpes, K., Kardara, M., Panousopoulos, G., Phillips, S. & Salamouras, S. (2009). Information exchange in business collaboration using grid technologies. *Identity in the Information Society, 2*(2), 189-204. doi: 10.1007/s12394-009-0028-0

Albrecht, W.S. & Albrecht, C. (2004). *Fraud examination & prevention*. Mason, Ohio: Thomson South-Western.

Alvesson, M. & Sveningsson, S. (2008). *Changing organizational culture: cultural change work in progress*. Retrieved from http://untag-smd.ac.id/files/Perpustakaan_Digital_2/ORGANIZATIONAL%20CULTURE%20Changing%20Organizational.pdf

Appleton, J.V. (2002). Critiquing approaches to case study design for a constructivist inquiry. *Qualitative Research Journal, 2*(2), 80-97. Retrieved from http://www.aqr.org.uk

Ardichvili, A., Page, V. & Wentling, T. (2003). Motivation and barriers to participation in virtual knowledge-sharing communities of practice. *Journal of Knowledge Management, 7*(1), 64-77. doi: 10.1108/13673270310463626

Argote, L. & Ingram, P. (2000). Knowledge transfer: a basis for competitive advantage in firms. *Organizational Behaviour and Human Decision Processes, 82*(1), 150-169. doi: 10.1006/obhd.2000.2893

Argote, L., Ingram, P., Levine, J.M. & Moreland, R.L. (2000). Knowledge transfer in organizations: learning from the experience of others. *Organizational Behaviour and Human Decision Processes, 82*(1), 1-8. doi: 10.1006/obhd.2000.2883

Association of Certified Fraud Examiners. (2016). *Report to the nations on occupational fraud and abuse: 2016 global fraud study.* Austin: ACFE.

Association of Certified Fraud Examiners. (2014). *Report to the nations on occupational fraud and abuse: 2014 global fraud study.* Austin: ACFE.

Association of Certified Fraud Examiners. (2012). *Report to the nations on occupational fraud and abuse: 2012 global fraud study.* Austin: ACFE.

Association of Certified Fraud Examiners. (2010). *Report to the nations on occupational fraud and abuse: 2010 global fraud study.* Austin: ACFE.

Association of Chief Police Officers. (2005). *Guidance on the national intelligence model*. Retrieved from the National Archives website: http://webarchive.nationalarchives.gov.uk/20090210103312/http://www.acpo.police.uk/asp/policies/Data/nim2005.pdf

Audit Commission. (2014). *National Fraud Initiative: national report 2014*. Retrieved from the Cabinet Office website: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/400955/NFI-national-report-FINAL-11-June-2014.pdf

Bachman, R. & Schutt, R.K. (2007). *The practice of research in criminology and criminal justice* (3rd ed.). Thousand Oaks, California: SAGE.

Bajaj, A. & Ram, S. (2007). A comprehensive framework towards information sharing between government agencies. *International Journal of Electronic Government Research, 3*(2), 29-44. doi: 10.4018/jegr.2007040102

Bandler, J. & Varchaver, N. (2009, April 30). How Bernie did it. *Fortune*. Retrieved from http://archive.fortune.com/2009/04/24/news/newsmakers/madoff.fortune/index.htm

Barker, S. (2012, October 25). The interview: crime stoppers. *Insurance Times*, 20-21.

Bazeley, P. (2009). Analysing qualitative data: more than 'identifying themes'. *Malaysian Journal of Qualitative Research, 2*(2), 6-22. Retrieved from http://www.researchsupport.com.au/bazeley_mjqr_2009.pdf

Bazeley, P. & Jackson, K. (2013). *Qualitative data analysis with Nvivo* (2nd ed.). London: SAGE.

Bélanger, F. & Carter, L. (2008). Trust and risk in e-government adoption. *Journal of Strategic Information Systems, 17*(2), 165-176. doi: 10.1016/j.jsis.2007.12.002

Bellamy, C., 6, P. & Raab, C. (2005a). Joined-up government and privacy in the United Kingdom: managing tensions between data protection and social policy. Part II. *Public Administration, 83*(2), 393-415. doi: 10.1111/j.0033-3298.2005.00455.x

Bellamy, C., Raab, C. & 6, P. (2005b). Multi-agency working in British social policy: risk, information sharing and privacy. *Information Polity, 10*(1-2), 51-63. Retrieved from http://iospress.metapress.com/content/300389/?p=fd6b2f1ed94d4538bc273f2c47bdad94&pi=0

Bellinger, G., Castro, D., & Mills, A. (2004). *Data, information, knowledge, and wisdom*. Retrieved from http://geoffreyanderson.net/capstone/export/37/trunk/research/ackoffDiscussion.pdf

Bereska, T.M. (2003). How will I know a code when I see it? *Qualitative Research Journal, 3*(2), 60-74. Retrieved from http://www.aqr.org.uk

Bharosa, N., Lee, J. & Janssen, M. (2010). Challenges and obstacles in sharing and coordinating information during multi-agency disaster response: propositions from field exercises. *Information Systems Frontiers, 12*(1), 49-65. doi: 10.1007/s10796-009-9174-z

Bichard, M. (2004). *The Bichard inquiry report.* Retrieved from http://dera.ioe.ac.uk/6394/1/report.pdf

Boba, R., Weisburd, D. & Meeker, J.W. (2009). The limits of regional data sharing and regional problem solving: observations from the East Valley, CA COMPASS initiative. *Police Quarterly, 12*(1), pp 22-41. doi: 10.1177/1098611107309279

Bock, G-W., Zmud, R.W., Kim, Y-G. & Lee, J-N. (2005). Behavioural intention formation in knowledge sharing: examining the roles of extrinsic motivators, social-psychological forces, and organizational climate. *MIS Quarterly, 29*(1), 87-111. Retrieved from www.jstor.org/stable/25148669

Brady, H. (2008). Europol and the European criminal intelligence model: a non-state response to organized crime. *Policing, 2*(1), 103-101. doi: 10.1093/police/pan014

Brazelton, J. & Gorry, G.A. (2003). Creating a knowledge-sharing community: if you build it, will they come? *Communications of the ACM, 46*(2), 23-25. Retrieved from http://cacm.acm.org/

Brinkmann, S. & Kvale, S. (2005). Confronting the ethics of qualitative research. *Journal of Constructivist Psychology, 18*(2), 157-181. doi: 10.1080/10720530590914789

British Society of Criminology. (2015). *Statement of ethics 2015.* Retrieved from http://www.britsoccrim.org/documents/BSCEthics2015.pdf

British Sociological Association. (2002). *Statement of ethical practice for the British Sociological Association (March 2002)*. Retrieved from https://www.britsoc.co.uk/media/23902/statementofethicalpractice.pdf

Brooks, G., Button, M. & Frimpong, K. (2009). Policing fraud in the private sector: a survey of the FTSE 100 companies in the UK. *International Journal of Police Science & Management, 11*(4), 493-504. doi: *10.1350/ijps.2009.00.0.140*

Brooks, S., Moss, K. & Pease, K. (2003). Data-sharing and crime reduction: the long and winding road. *Crime Prevention & Community Safety: An International Journal, 5*(4), 7-14. doi: 10.1057/palgrave.cpcs.8140158

Brown, S.D. (2007). The meaning of criminal intelligence. *International Journal of Police Science & Management, 9*(4), 336-340. doi: 10.1350/ijps.2007.9.4.336

Bryman, A. (2012). *Social research methods* (4th ed.). Oxford: Oxford University Press.

Button, M. (2011). Fraud investigation and the 'flawed architecture' of counter fraud entities in the United Kingdom. *International Journal of Law, Crime and Justice, 39*(4), 249-265. doi: 10.1016/j.ijlcj.2011.06.001

Button, M. & Gee, J. (2013). *Countering fraud for competitive advantage: the professional approach to reducing the last great hidden cost*. Chichester: John Wiley & Sons.

Button, M., Johnston, L. & Frimpong, K. (2008). The fraud review and the policing of fraud: laying the foundations for a centralized fraud police or counter fraud executive? *Policing, 2*(2), 241-250. doi:10.1093/police/pan027

Cabinet Office. (2008). *Data handling procedures in government: final report*. Retrieved from the Cabinet Office website: http://www.cabinetoffice.gov.uk/sites/default/files/resources/final-report.pdf

Cabinet Office. (2011a). *Eliminating public sector fraud: the Cabinet Office Counter Fraud Taskforce interim report*. Retrieved from the Cabinet Office website: http://www.cabinetoffice.gov.uk/resource-library/eliminating-public-sector-fraud-counter-fraud-taskforce-interim-report

Cabinet Office. (2011b). *The UK cyber security strategy: protecting and promoting the UK in a digital world*. Retrieved from the Cabinet Office website: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

Cabinet Office. (2016). *National Fraud Initiative*. Retrieved from the Cabinet Office website: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/565216/nfi_national_report_2016.pdf

Cabrera, A. & Cabrera, E.F. (2002). Knowledge-sharing dilemmas. *Organization Studies, 23*(5), 687-710. doi: 10.1177/0170840602235001

Cabrera, A., Collins, W.C. & Salgado, J.F. (2006). Determinants of individual engagement in knowledge sharing. *The International Journal of Human Resource Management, 17*(2), 245-264. doi: 10.1080/09585190500404614

Calder, A. (2016). *EU GDPR: a pocket guide*. Ely: IT Governance Publishing.

Camilli, E. (2015). The Paris attacks. A case of intelligence failure? *NATO Review Magazine*. Retrieved from http://www.nato.int/docu/review/2015/ISIL/Paris-attacks-terrorism-intelligence-ISIS/EN/index.htm

Canestraro, D.S., Pardo, T.A., Raup-Kounovsky, A.N. & Taratus, D. (2009). Regional telecommunication incident coordination: sharing information for rapid response. *Information Polity, 14*(1-2), 113-126. doi: 10.3233/IP-2009-0166

Centre for Economics and Business Research. (2015). *The business and economic consequences of inadequate cybersecurity*. Retrieved from the Veracode website: https://info.veracode.com/analyst-report-cebr-business-and-economic-consequences-of-inadequate-cybersecurity.html

Chartered Insurance Institute New Generation Group. (2015). *Industry best practice guide: section 29(3) of the Data Protection Act 1998 v7.0*. Retrieved from the Insurance Fraud Bureau website: https://www.insurancefraudbureau.org/media/1091/section-29-3-best-practice-guide-v7.pdf

Chartered Institute of Public Finance and Accountancy. (2016). *Fighting fraud & corruption locally: the local government counter fraud and corruption strategy 2016-2019*. Retrieved from the Department for Communities and Local Government website: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/503657/Fighting_fraud_and_corruption_locally_strategy.pdf

Chatham House. (2017). *Chatham House rule*. Retrieved from https://www.chathamhouse.org/about/chatham-house-rule

Chau, M., Atabakhsh, H., Zeng, D. & Chen, H. (2001). *Building an infrastructure for law enforcement information sharing and collaboration: design issues and challenges*. Retrieved from http://arizona.openrepository.com/arizona/bitstream/10150/105531/1/chau4.pdf

Chen, H., Schroeder, J., Hauck, R.V., Ridgeway, L., Atabakhsh, H., Gupta, H., Boarman, C., Rasmussen, K. & Clements, A.W. (2002). COPLINK Connect: information and knowledge management for law enforcement. *Decision Support Systems, 34*(3), 271-285. doi: 10.1016/S0167-9236(02)00121-5

Chen, H., Wang, F-Y. & Zeng, D. (2004). Intelligence and security informatics for homeland security: information, communication and transportation. *IEEE Transactions on Intelligence Transportation Systems, 5*(4), 329-341. doi: 10.1109/TITS.2004.837824

Chun, S.A., Luna-Reyes, L.F. & Sandoval-Almazán, R. (2012). Collaborative e-government. *Transforming Government: People, Process & Policy, 6*(1), 5-12. doi: 10.1108/17506161211214868

City of London Police. (2010). *General guide to the NFIB: information for data providers and the public*. Retrieved from the National Fraud Authority website: http://www.homeoffice.gov.uk/publications/agencies-public-bodies/nfa/general-guide-nfib?view=Binary

City of London Police. (2012). *Information sharing protocol: National Fraud Intelligence Bureau*. Unpublished internal document: City of London Police.

Clarkson, G., Jacobsen, T.E. & Batcheller, A.L. (2007). Information asymmetry and information sharing. *Government Information Quarterly, 24*(4), 827-839. doi: 10.1016/j.giq.2007.08.001

Clausewitz, C. v. (1989). *On war* (M. Howard & P. Paret, Trans.). Chichester: Princeton University Press. (Original work published 1832)

Clements, P. & Jones, J. (2008). *The diversity training handbook* (3rd ed.). Retrieved from https://ebookcentral.proquest.com/lib/portsmouth-ebooks/detail.action?docID=408675

Coleman, N. (2008). *Protecting government information: independent review of government information assurance. The Coleman report*. London: Cabinet Office. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60967/ia_review.pdf

College of Policing. (2015a). *About us*. Retrieved from the College of Policing website: http://www.college.police.uk/About/Pages/default.aspx

College of Policing. (2015). *Intelligence report*. Retrieved from https://www.app.college.police.uk/app-content/intelligence-management/intelligence-report/

Comer. M. (2003). *Investigating corporate fraud*. Aldershot: Gower.

Constant, D., Kiesler, S. & Sproull, L. (1994). What's mine is ours, or is it? A study of attitudes about information sharing. *Information Systems Research, 5*(4), 400-421. Retrieved from http://isr.journal.informs.org/

Cooper, D.P. (2005). Investigations: understanding data privacy. *Journal of Financial Crime, 12*(4), 352-359. doi: 10.1108/13590790510700571

Cope, N. (2004). 'Intelligence led policing or policing led intelligence?': integrating volume crime analysis into policing. *British Journal of Criminology, 44*(2), 188-203. doi: 10.1093/bjc/44.2.188

Corera, G. (2016, January 01). Why intelligence sharing still has a long way to go. *British Broadcasting Corporation*. Retrieved from http://www.bbc.co.uk/news/world-europe-35154640

Corfield, A. & Paton, R. (2016). Investigating knowledge management: can KM really change organisational culture? *Journal of Knowledge Management, 20*(1), 88-103. doi: 10.1108/JKM-12-2014-0502

Coyne, I.T. (1997). Sampling in qualitative research. Purposeful and theoretical sampling; merging or clear boundaries? *Journal of Advanced Nursing, 26*(3), 623-630. doi: 10.1046/j.1365-2648.1997.t01-25-00999.x

Cress, U., Kimmerle, J. & Hesse, F.W. (2006). Information exchange with shared databases as a social dilemma: the effect of metaknowledge, bonus systems, and costs. *Communication Research, 33*(5), 370-390. doi: 10.1177/0093650206291481

Cresswell, A.M., Pardo, T.A., Canestraro, D.S. & Dawes, S.S. (2005). *Why assess information sharing capability?* Retrieved from http://demo.ctg.albany.edu/publications/guides/why_assess/why_assess.pdf

Cresswell, A.M., Pardo, T.A. & Hassan, S. (2007). Assessing capability for justice information sharing. *The Proceedings of the 8th Annual International Digital Government Research Conference*. Retrieved from http://dl.acm.org/citation.cfm?id=1248479

Cresswell, J.W. & Tashakkori, A. (2007). Editorial: differing perspectives on mixed methods research. *Journal of Mixed Methods Research, 1*(4), 303-308. doi: 10.1177/1558689807306132

Creswell, J.W. (2009). *Research design: qualitative, quantitative and mixed methods approaches* (3rd ed.). Thousand Oaks, California: SAGE.

Darke, P., Shanks, G. & Broadbent, M. (1998). Successfully completing case study research: combining rigour, relevance and pragmatism. *Information Systems Journal, 8*(4), 273-289. doi: 10.1046/j.1365-2575.1998.00040.x

Davies, P. (2011). Doing interviews in prison. In P. Davies, P. Francis & V. Jupp (Eds.), *Doing criminological research* (2nd ed.) (pp.161-178). London: SAGE.

Davies, P. & Francis, P. (2011). Reflecting on criminological research. In P. Davies, P. Francis & V. Jupp (Eds.), *Doing criminological research* (2nd ed.) (pp.281-285). London: SAGE.

Davies, P.H.J., Gustafson, K. & Rigden, I. (2013). The intelligence cycle is dead, long live the intelligence cycle: rethinking intelligence fundamentals for a new intelligence doctrine. In M. Phythian (Ed.), *Understanding the intelligence cycle* (pp.56-75). Abingdon: Routledge.

Dawes, R.M. (1980). Social dilemmas. *Annual Review of Psychology, 31*, 169-193. doi: 10.1146/annurev.ps.31.020180.001125

Dawes, S.S. (1996). Interagency information sharing: expected benefits, manageable risks. *Journal of Policy Analysis and Management, 15*(3), 377-394. doi: 10.1002/(SICI)1520-6688(199622)15:3<377::AID-PAM3>3.0.CO;2-F

Dawes, S.S., Cresswell, A.M. & Pardo, T.A. (2009). From "need to know" to "need to share": tangled problems, information boundaries, and the building of public sector knowledge networks. *Public Administration Review, 69*(3), 392-402. doi: 10.1111/j.1540-6210.2009.01987_2.x

De Lange, P., Jackling, B. & Suwardy, T. (2015). Continuing professional development in the accounting profession: practices and perceptions from the Asia Pacific region. *Accounting Education, 24*(1), 41-56. doi: 10.1080/09639284.2014.1002800

Degwekar, S., DePree, J., Beck, H., Thomas, C.S. & Su, S.Y.W. (2007). Event-triggered data and knowledge sharing among collaborating government organizations. *The Proceedings of the 8th Annual International Digital Government Research Conference*. Retrieved from http://dl.acm.org/citation.cfm?id=1248477

Denscombe, M. (2007). *The good research guide for small-scale research projects* (3rd ed.). Maidenhead: Open University Press.

Denscombe, M. (2010). *Ground rules for social research: guidelines for good practice* (2nd ed.). Maidenhead: Open University Press.

Department for Constitutional Affairs. (2011). *Public sector data sharing: guidance on the law*. Retrieved from the Ministry of Justice website: http://www.justice.gov.uk/downloads/information-access-rights/data-sharing/annex-h-data-sharing.pdf

Devers, K.J. & Frankel, R.M. (2000). Study design in qualitative research–2: sampling and data collection strategies. *Education for Health, 13(*2), 263-271. doi: 10.1080/13576280050074543

DiCicco-Bloom, B. & Crabtree, B.F. (2006). The qualitative research interview. *Medical Education, 40*(4), 314-321. doi: 10.1111/j.1365-2929.2006.02418.x

Doig, A. (2006). *Fraud*. Cullompton: Willan.

Doig, A. & Levi, M. (2009). Inter-agency work and the UK public sector investigation of fraud, 1996-2006: joined-up rhetoric and disjointed reality. *Policing and Society: An International Journal of Research and Policy, 19*(3), 199-215. doi: 10.1080/10439460902863311

Drake, D.B., Steckler, N.A. & Koch, M.J. (2004). Information sharing in and across government agencies: the role and influence of scientist, politician and bureaucrat subcultures. *Social Science Computer Review, 22*(1), 67-84. doi: 10.1177/0894439303259889

Dunne, M., Pryor, J. & Yates, P. (2005). *Becoming a researcher: a research companion for the social sciences*. Maidenhead: Open University Press.

Edgley, C., Sharma, N. & Anderson-Gough, F. (2016). Diversity and professionalism in the Big Four firms: expectation, celebration and weapon in the battle for talent. *Critical Perspectives on Accounting, 35*(2016), 13-34. doi: 10.1016/j.cpa.2015.05.005

Evans, G. (2009). Rethinking military intelligence failure – putting the wheels back on the intelligence cycle. *Defence Studies, 9*(1), 22-46. doi: 10.1080/14702430701811987

Evetts, J. (1999). Professionalisation and professionalism: issues for interprofessional care. *Journal of Interprofessional Care, 13*(2), 119-128. doi: 10.3109/13561829909025544

Evetts, J. (2003). The sociological analysis of professionalism: occupational change in the modern world. *International Sociology, 18*(2), 395-415. doi: 10.1177/0268580903018002005

Evetts, J. (2006a). Short note: the sociology of professional groups: new directions. *Current Sociology, 54*(1), 133-143. doi*: 10.1177/0011392106057161*

Evetts, J. (2006b). Trust and professionalism: challenges and occupational changes. *Current Sociology, 54*(4), 515-531. doi:

Evetts, J. (2011). A new professionalism? Challenges and opportunities. *Current Sociology, 59*(4), 406-422. doi: 10.1177/0011392111402585

Evetts, J. (2013). Professionalism: value and ideology. *Current Sociology, 61*(5-6), 778-796. doi: 10.1177/0011392113479316

Farrell, S., Yeo, N. & Ladenburg, G. (2007). *Blackstone's guide to the Fraud Act 2006*. Oxford: Oxford University Press.

Federation Against Copyright Theft. (n.d.). *Protecting IP: benefits of FACT membership*. Old Isleworth: Federation Against Copyright Theft.

Federation Against Copyright Theft. (1982). *Untitled*. Retrieved from https://s3-eu-west-1.amazonaws.com/documentNameChangeDocuments

Federation Against Copyright Theft. (2008). *Joint working intelligence initiative between The Federation Against Copyright Theft (UK) and Gatwick Divisional Intelligence Unit*. Unpublished internal document: Federation Against Copyright Theft.

Federation Against Copyright Theft. (2012a). *Camcording & illegal recording: best practices to prevent film theft (revised 2012)*. Old Isleworth: Federation Against Copyright Theft.

Federation Against Copyright Theft. (2012b). *Strategic assessment 2012*. Unpublished internal document, Federation Against Copyright Theft.

Federation Against Copyright Theft. (2013a). *FACT 30 Years: protecting IP for 30 years*. Old Isleworth: Federation Against Copyright Theft.

Federation Against Copyright Theft. (2013b, September). *Operational plan 2014 v1*. Unpublished internal document, Federation Against Copyright Theft.

Federation Against Copyright Theft. (2013c). *Strategic assessment 2013*. Unpublished internal document: Federation Against Copyright Theft.

Federation Against Copyright Theft. (2014). *Report and Financial Statements*. Retrieved from https://s3-eu-west-1.amazonaws.com/documentAnnualReport2014

Federation Against Copyright Theft. (2015a). *About FACT*. Retrieved from http://www.fact-uk.org.uk/about-fact/

Federation Against Copyright Theft. (2015b). *Online movie release group sentenced to over 17 years*. Retrieved from https://www.fact-uk.org.uk/online-movie-release-group-sentenced-to-over-17-years/

Federation Against Copyright Theft. (2016a). *Certificate of Passing* [and] *Articles of Association*. Retrieved from https://s3-eu-west-1.amazonaws.com/documentArticlesofAssociation2016

Federation Against Copyright Theft. (2016b). *FACT Certified Directory*. Retrieved from http://www.factcertification.com/?page_id=11

Federation Against Copyright Theft. (2016c). *FACT launches services outside of audio-visual industry*. Retrieved from https://www.fact-uk.org.uk/fact-launches-services-outside-of-audio-visual-industry/

Federation Against Copyright Theft. (2016d). *Members*. Retrieved from https://www.fact-uk.org.uk/about-fact/members/

Federation Against Copyright Theft. (2016e). *Post Office manager jailed over fake DVD business*. Retrieved from https://www.fact-uk.org.uk/post-office-manager-jailed-over-fake-dvd-business/

Federation Against Copyright Theft. (2016f). *Two Leeds pubs convicted and ordered to pay more than £8,500 for illegal Sky use*. Retrieved from https://www.fact-uk.org.uk/two-pub-licencees-in-leeds-convicted-and-ordered-to-pay-more-than-8500-for-illegal-sky-use/

Fedorowicz, J., Gogan, J.L. & Williams, C.B. (2007). A collaborative network for first responders: lessons from the CapWIN case. *Government Information Quarterly, 24*(4), 785-807. doi: 10.1016/j.giq.2007.06.001

Fighting Fraud Locally Oversight Board. (2011). *Fighting fraud locally: the local government fraud strategy*. Retrieved from the National Fraud Authority website: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/118508/strategy-document.pdf

Flyvberg, B. (2006). Five misunderstandings about case study research. *Qualitative Inquiry, 12*(2), 219-245. doi: 10.1177/1077800405284363.

Frankel, R.M. & Devers, K.J. (2000). Study design in qualitative research–1: developing questions and assessing resource needs. *Education for Health, 13*(2), 251-261. Retrieved from http://www.educationforhealth.net/home/defaultnew.asp

Fraud Advisory Panel. (2016). *The fraud review: ten years on*. Retrieved from the Fraud Advisory Panel website: https://www.fraudadvisorypanel.org/wp-content/uploads/2016/06/The-Fraud-Review-Ten-Years-On-WEB.pdf

Fraud Review Team. (2006a). *Fraud review team: interim report*. Retrieved from the Northumberland County Council website: http://www2.northumberland.gov.uk/reports/anti-fraud/Documents/General/Interim_Fraud_Report_03_06.pdf

Fraud Review Team. (2006b). *Fraud review: final report.* Retrieved from Attorney General's website: www.attorneygeneral.gov.uk/Fraud%20Review%20Final%20Report%20July%202006.pdf

Freidson, E. (1989). Theory and the professions. *Indiana Law Journal, 64*(3), 423-432. Retrieved from http://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1199&context=ilj

Frontier Economics. (2011). *Estimating the global economic and social impacts of counterfeiting and piracy*. Retrieved from the International Chamber of Commerce website: http://www.iccwbo.org/Advocacy-Codes-and-Rules/BASCAP/BASCAP-Research/Economic-impact/Global-Impacts-Study/

Gil-Garcia, J.R., Chengalur-Smith, I. & Duchessi, P. (2007). Collaborative e-government: impediments and benefits of information-sharing projects in the public sector. *European Journal of Information Systems, 16*(2), 121-133. doi: 10.1057/palgrave.ejis.3000673

Gil-Garcia, J.R., Chun, S.A. & Janssen, M. (2009). Government information sharing and integration: combining the social and the technical. *Information Polity, 14*(1-2), 1-10. doi: 10.3233/IP-2009-0176

Gil-Garcia, J.R. & Pardo, T.A. (2005). E-government success factors: mapping practical tools to theoretical foundations. *Government Information Quarterly, 22*(2), 187-216. doi: 10.1016/j.giq.2005.02.001

Gil-Garcia, J.R., Schneider, C.A., Pardo, T.A. & Cresswell, A.M. (2005). Interorganizational information integration in the criminal justice enterprise: preliminary lessons from state and county initiatives. *Proceedings of the 38th Hawaii Conference on System Sciences*. Retrieved from http://dl.acm.org/citation.cfm?id=1042436.1042937

Gill, P. & Phythian, M. (2013). From intelligence cycle to web of intelligence: complexity and the conceptualisation of intelligence. In M. Phythian (Ed.), *Understanding the intelligence cycle* (pp.21-42). Abingdon: Routledge.

Gladwell, M. (2007, January 08). Open secrets: the mystery of Enron. *New Yorker*. Retrieved from http://www.newyorker.com/magazine/2007/01/08/open-secrets-3

Glaser, B.G. (1965). The constant comparative method of qualitative analysis. *Social Problems, 12*(4), 436-445. doi: 10.2307/798843

Glaser, B.G. & Strauss, A.L. (1967). *The discovery of grounded theory: strategies for qualitative research*. New Jersey: AldineTransaction.

Gorard, S. (2003). Quantitative methods in social science: the role of numbers made easy. London: Continuum.

Gottschalk, P. (2005). Expert systems at stage iv of the knowledge management technology stage model: the case of police investigations. *Expert Systems with Applications, 31*(3), 617-628. doi: 10.1016/j.eswa.2005.09.063

Gottschalk, P. (2006). Stages of knowledge management systems in police investigations. *Knowledge-Based Systems, 19*(6), 381-387. doi: 10.1016/j.knosys.2006.04.002

Grabiner, A.S. (2000). *The informal economy*. London: The Stationary Office. Retrieved from http://webarchive.nationalarchives.gov.uk/20060213220418/http://www.hm-treasury.gov.uk/media/DE3/8E/74.pdf

Grix, J. (2010). *The foundations of research* (2nd ed.). Basingstoke: Palgrave Macmillan.

Hagan, F.E. (1982). *Research methods in criminal justice and criminology.* New York: Macmillan.

Handy, C. (1993). *Understanding organisations* (4th ed.). London: Penguin.

Hardouin, P. (2009). Banks governance and public-private partnership in preventing and confronting organized crime, corruption and terrorism financing. *Journal of Financial Crime, 16*(3), 199-209. doi: 10.1108/13590790910971757

Hart, C. (1998). *Doing a literature review: releasing the social science research imagination*. London: SAGE.

Hatala, J-P. & Lutta, J.G. (2009). Managing information sharing within an organizational setting: a social network perspective. *Performance Improvement Quarterly, 21*(4), 5-33. doi: 10.1002/piq.20036

Heaton, R. (2000). The prospects for intelligence-led policing: some historical and quantitative considerations. *Policing and Society: An International Journal of Research and Policy, 9*(4), 337-355. doi: 10.1080/10439463.2000.9964822

Heidensohn, F. (2008). International comparative research in criminology. In R.D. King & E. Wincup (Eds.), *Doing research on crime and justice* (2nd ed.) (pp.199-228). Oxford: Oxford University Press.

Heller, R. (2002). Making cultures behave. In L. Carden (Ed.), *Business: the ultimate resource*. London: Bloomsbury.

Her Majesty's Inspectorate of Constabulary. (1997). *Policing with intelligence: criminal intelligence – a thematic inspection on good practice*. Retrieved from the National Archives website: http://www.nationalarchives.gov.uk/ERORecords/HO/421/2/hmic/pintell.htm

HM Government. (2016). *Digital Economy Bill: explanatory notes*. Retrieved from the UK Parliament website: http://www.publications.parliament.uk/pa/bills/cbill/2016-2017/0045/en/17045en.pdf

HM Treasury & National Audit Office. (2008). *Good practice guide: tackling external fraud*. Retrieved from the National Audit Office website: https://www.nao.org.uk/report/good-practice-in-tackling-external-fraud-2/

Home Office. (2011). *The National Crime Agency: a plan for the creation of a national crime-fighting capability*. Retrieved from Home Office, Publications website: http://www.homeoffice.gov.uk/publications/crime/nca-creation-plan?view=Binary

Home Office. (2013). *Serious and organised crime strategy*. Retrieved from the Home Office website: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/248645/Serious_and_Organised_Crime_Strategy.pdf

Home Office. (2015). *Data sharing for the prevention of fraud: code of practice for public authorities disclosing information to a specified anti-fraud organisation under sections 68-72 of the Serious Crime Act 2007*. Retrieved from the Home Office website: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/415469/Data_Sharing_for_the_Prevention_of_Fraud_-_Code_of_Practice__web_.pdf

Hughes, J.A. & Sharrock, W.W. (1997). *The philosophy of social research* (3rd ed.). Harlow: Pearson Education.

Hulnick, A.S. (2006). What's wrong with the intelligence cycle. *Intelligence and National Security, 21*(6), 959-979. doi: 10.1080/02684520601046291

Hulnick, A.S. (2013). Intelligence theory: seeking better models. In M. Phythian (Ed.), *Understanding the intelligence cycle* (pp.149-160). Abingdon: Routledge.

Information Commissioner's Office. (2001). *The data protection act 1998: legal guidance.* Wilmslow: Information Commissioner's Office.

Information Commissioner's Office. (2011). *Data sharing code of practice*. Retrieved from the Information Commissioner's Office website: https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf

Information Commissioner's Office. (2012). *Anonymisation: managing data protection risk. Code of practice*. Retrieved from the Information Commissioner's Office website: https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf

Information Commissioner's Office. (2015a). *ICO review: data sharing between the public and private sector to prevent fraud*. Retrieved from the Information Commissioner's Office website: https://ico.org.uk/media/action-weve-taken/audits-and-advisory-visits/1043719/ico-review-data-sharing-to-prevent-fraud.pdf

Information Commissioner's Office. (2015b). *Using the crime and taxation exemptions: Data Protection Act*. Retrieved from the Information Commissioner's Office website: https://ico.org.uk/media/1594/section-29.pdf

Information Commissioner's Office. (2016). *Overview of the General Data Protection Regulation (GDPR)*. Retrieved from the Information Commissioner's Office website: https://ico.org.uk/media/for-organisations/data-protection-reform/overview-of-the-gdpr-1-1.pdf

IP Crime Group. (2014). *IP crime report 2013/14*. Retrieved from the Intellectual Property Office website: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374283/ipcreport13.PDF

IP Crime Group. (2015). *IP crime report 2014/15*. Retrieved from the Intellectual Property Office website: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/461792/ip-crime-report-2014-15.pdf

IP Commission. (2013). *The IP Commission report: the report of The Commission on the Theft of American Intellectual Property*. Retrieved from the Commission on the Theft of American Intellectual Property website: http://www.ipcommission.org/report/ip_commission_report_052213.pdf

Ipe, M. (2003). Knowledge sharing in organizations: a conceptual framework. *Human Resource Development Review, 2*(4), 337-359. doi: 10.1177/1534484303257985

James, A. (2013). *Examining intelligence-led policing: developments in research, policy and practice*. Basingstoke: Palgrave Macmillan.

James, A. (2016). *Understanding police intelligence work*. Bristol: Policy Press.

Jarvenpaa, S.L. & Staples, D.S. (2000). The use of collaborative electronic media for information sharing: an exploratory study of determinants. *Strategic Information Systems, 9*(2-3), 129-154. doi: 10.1016/S0963-8687(00)00042-1

Jarvenpaa, S.L. & Staples, D.S. (2001). Exploring perceptions of organizational ownership of information and expertise. *Journal of Management Information Systems, 18*(1), 151-183. Retrieved from http://www.jmis-web.org/

Jennex, M. E. (2009). Re-visiting the knowledge pyramid. *HICSS '09. 42nd Hawaii International Conference On System Sciences, 42,* pp. 1-7. doi: 10.1109/HICSS.2009.361

John, T. & Maguire, M. (2004a). *The national intelligence model: early implementation experience in three police force areas*. Retrieved from https://orca-mwe.cf.ac.uk/78093/1/wrkgpaper-50.pdf

John, T. & Maguire, M. (2004b). *The national intelligence model: key lessons from early research*. Retrieved from the ResearchGate website: https://www.researchgate.net/publication/242484328_The_National_Intelligence_Model_key_lessons_from_early_research

John, T. & Maguire, M. (2007). Criminal intelligence and the National Intelligence Model. In T. Newburn, T. Williamson & A. Wright (Eds.), *Handbook of criminal investigation* (pp.199-225). Retrieved from https://ebookcentral.proquest.com/lib/portsmouth-ebooks/reader.action?docID=449559&ppg=226

Johnson, L. (2003). Bricks and mortar for a theory of intelligence. *Comparative Strategy, 22*(1), 1-28. doi: 10.1080/01495930390130481

Johnson, L. K. (2016). A framework for strengthening U.S. intelligence. *Yale Journal of International Affairs, 1*(2), pp.116-131. Retrieved from http://yalejournal.org/

Johnson, R.B. & Onwuegbuzie, A.J. (2004). Mixed methods research: a research paradigm whose time has come. *Educational Researcher, 33*(7), 14-26. doi: 10.3102/0013189X033007014

Johnson, R.B., Onwuegbuzie, A.J. & Turner, L.A. (2007). Towards a definition of mixed methods research. *Journal of Mixed Methods Research, 1*(2), 112-133. doi: 10.1177/1558689806298224

Juniper Research. (2015). *Cybercrime and the internet of threats*. Retrieved from the Juniper Research website: http://www.juniperresearch.com/document-library/white-papers/cybercrime-the-internet-of-threats

Kalman, M.E., Monge, P., Fulk, J. & Heino, R. (2002). Motivations to resolve communication dilemmas in database-mediated collaboration. *Communication Research, 29*(2), 125-154. doi: 10.1177/0093650202029002002

Karagiannis, E. (2017, March 15). *Were the attacks in Paris and Brussels an intelligence failure?* [Web log message]. Retrieved from https://defenceindepth.co/2017/03/15/were-the-attacks-in-paris-and-brussels-an-intelligence-failure/

Kennedy, A. (2007). Winning the information wars: collecting, sharing and analysing information in asset recovery investigations. *Journal of Financial Crime, 14*(4), 372-404. doi: 10.1108/13590790710828136

Kezar, A. (2000). The importance of pilot studies: beginning the hermeneutic circle. *Research in higher education, 41*(3), 385-400. doi: 10.1023/A:1007047028758

Kim, S. & Lee, H. (2006). The impact of organizational context and information technology on employee knowledge-sharing capabilities. *Public Administration Review, 66*(3), 370-385. doi: 10.1111/j.1540-6210.2006.00595.x

Kirby, S. & McPherson, I. (2004). Integrating the national intelligence model with a 'problem solving approach'. *Community Safety Journal, 3*(2), 36-46. doi: 10.1108/17578043200400014

Kleiven, M.E. (2007). Where's the intelligence in the national intelligence model? *International Journal of Police Science & Management, 9*(3), 257-273. doi: 10.1350/ijps.2007.9.3.257

Klischewski, R. & Scholl, H.J. (2006). Information quality as a common ground for key players in e-government integration and interoperability. *Proceedings of the 39th Hawaii Conference on System Sciences*. Retrieved from http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1579433

Kolekofski Jr., K.E. & Heminger, A.R. (2003). Beliefs and attitudes affecting intentions to share information in an organizational setting. *Information & Management, 40*(6), 521-532. doi: 10.1016/S0378-7206(02)00068-X

Kreuzer, M.P. (2016). Professionalizing intelligence analysis: an expertise and responsibility centered approach. *Intelligence and National Security, 31*(4), 579-597. doi: 10.1080/02684527.2015.1039228

Kvale, S. & Brinkmann, S. (2009). *Interviews: learning the craft of qualitative research interviewing* (2nd ed.). Thousand Oaks: SAGE.

Landsbergen, D. & Wolken, G. (1998). *Eliminating legal and policy barriers to interoperable government systems: Phase II: Recommendations*. Retrieved from https://osc.edu/files/press/releases/1998/phase_2_Recommendations.pdf

Landsbergen, Jr., D. & Wolken, Jr., G. (2001). Realizing the promise: government information systems and the fourth generation of information technology. *Public Administration Review, 61*(2), 206-220. Retrieved from http://www.jstor.org/stable/977454

Lam, W. (2005). Barriers to e-government integration. *The Journal of Enterprise Information Management, 18*(5), 511-530. doi: 10.1108/17410390510623981

Law Commission. (2002). Fraud: report on a reference under section 3(1)(e) of the Law Commissions Act 1965. Retrieved from the Law Commission website: http://www.lawcom.gov.uk/wp-content/uploads/2015/03/lc276_Fraud.pdf

Law Commission. (2013). *Data sharing between public bodies: a consultation paper*. Retrieved from the Law Commission website: http://www.lawcom.gov.uk/wp-content/uploads/2015/03/cp214_data-sharing.pdf

Law Commission. (2014). Data sharing between public bodies: a scoping report. Retrieved from the Law Commission website: http://www.lawcom.gov.uk/wp-content/uploads/2015/03/lc351_data-sharing.pdf

Lazer, D. & Binz-Scharf, M. (2004). *Information sharing in e-government projects: managing novelty and cross-agency cooperation*. Retrieved from http://www.umass.edu/digitalcenter/research/pdfs/IBM_lazer_binz-scharf.pdf

Lee, J. & Rao, H.R. (2007). Exploring the causes and effects of inter-agency information sharing systems adoption in the anti/counter-terrorism and disaster management domains. *The Proceedings of the 8th Annual International Digital Government Research Conference.* Retrieved from http://dl.acm.org/citation.cfm?id=1248485

Levi, M. (1987). Regulating fraud: white-collar crime and the criminal process. London: Tavistock.

Levi, M. (2010). Public and private policing of financial crimes: the struggle for co-ordination. *Journal of Criminal Justice and Security*. Vol. 12, No. 4, pp 343-354. Retrieved from http://www.fvv.uni-mb.si/rV/revija-E.html

Levi, M., Burrows, J., Fleming, M.H. & Hopkins, M. (2007). *The nature, extent and economic impact of fraud in the UK*. Retrieved from the Association of Chief Police Officers website: http://www.acpo.police.uk/asp/policies/Data/Fraud%20in%20the%20UK.pdf

Levi, M. & Wall, D.S. (2004). Technologies, security and privacy in the post-9/11 European information society. *Journal of Law and Society, 31*(2), 194-220. doi: 10.1111/j.1467-6478.2004.00287.x

Li, S. & Lin, B. (2006). Accessing information sharing and information quality in supply chain management. *Decision Support Systems, 42*(3), 1641-1656. doi: 10.1016/j.dss.2006.02.011

Limwichitr, S. & Broady-Preston, J. (2015). A discussion of problems in implementing organisational cultural change: developing a learning organisation in university libraries. *Library Review, 64*(6/7), 480-488. doi: 10.1108/LR-10-2014-0116

Linder, A. (Ed.). (2016). *European Data Protection Law: General Data Protection Regulation 2016*. Great Britain: CreateSpace.

Luna-Reyes, L.F., Gil-Garcia, J.R. & Cruz, C.B. (2007). Collaborative digital government in Mexico: some lessons from federal web-based interorganizational information integration initiatives. *Government Information Quarterly, 24*(4), 808-826. doi: 10.1016/j.giq.2007.04.003

Macfarlane, B. (2009). *Researching with integrity: what does it really mean to be an ethical researcher?* Retrieved from University of Portsmouth, Victory Research Methods Hub website: https://victory.port.ac.uk/webct/urw/lc5116011.tp0/cobaltMainFrame.dowebct

Magee, I. (2008). *The review of criminality information*. London: Home Office. Retrieved from http://webarchive.nationalarchives.gov.uk/20080901210549/http://police.homeoffice.gov.uk/publications/operational-policing/roci-full-report?view=Binary

Maguire, M. (2000). Policing by risks and targets: some dimensions and implications of intelligence-led crime control. *Policing and Society: An International Journal of Research and Policy, 9*(4), 315-336. doi: 10.1080/10439463.2000.9964821

Maguire, M. & John, T. (2006). Intelligence led policing, managerialism and community engagement: competing priorities and the role of the National Intelligence Model in the UK. *Policing and Society: An International Journal of Research and Policy, 16*(1), 67-85. doi: 10.1080/10439460500399791

Malterud, K. (2001). Qualitative research: standards, challenges and guidelines. *The Lancet, 358*(9280), 483-488. doi: 10.1016/S0140-6736(01)05627-6

Manchester Safeguarding Children Board. (n.d.). *5x5x5 intelligence report template*. Retrieved from www.manchesterscb.org.uk/displaydoc.asp?id=466

Markopolos, H. (2010). *No one would listen: a true financial thriller*. New Jersey: John Wiley & Sons.

Marshall, H. (2002). What do we do when we code data? *Qualitative Research Journal, 2*(1), pp.56-70. Retrieved from http://www.agr.org.uk

Marshall, M.N. (1996). Sampling for qualitative research. *Family Practice, 13*(6), 522-525. doi: 10.1093/fampra/13.6.522

Metropolitan Police. (2012). *Purpose specific information sharing agreement*. Unpublished internal document: Metropolitan Police.

Miranda, S.M. & Saunders, C.S. (2003). The social construction of meaning: an alternative perspective on information sharing. *Information Systems Research, 14*(1), 87-106. doi: 10.1287/isre.14.1.87.14765

Moss, K. & Pease, K. (2004). Data sharing in crime prevention: why and how. *Crime Prevention and Community Safety: An International Journal, 6*(1), 7-12. doi: 10.1057/palgrave.cpcs.8140175

Muzio, D., Brock, D.M. & Suddaby, R. (2013). Professions and institutional change: towards an institutionalist sociology of the professions. *Journal of Management Studies, 50*(5), 699-721. doi: 10.1111/joms.12030

Myers, M.D. & Newman, M. (2007). The qualitative interview in IS research: examining the craft. *Information and Organization, 17*(1), 2-26. doi: 10.1016/j.infoandorg.2006.11.001

National Audit Office. (n.d.). *A practical guide to sampling.* Retrieved from https://www.nao.org.uk/wp-content/uploads/2001/06/SamplingGuide.pdf

National Audit Office. (2015). *Fraud and error stocktake*. Retrieved from the National Audit Office website: https://www.nao.org.uk/wp-content/uploads/2015/07/Fraud-and-error-stocktake.pdf

National Audit Office. (2016). *Fraud landscape review*. Retrieved from the National Audit Office website: https://www.nao.org.uk/wp-content/uploads/2016/02/Fraud-landscape-review.pdf

National Commission on Terrorist Attacks Upon the United States. (2004). *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States: Authorized Edition.* New York: Norton.

National Crime Agency. (2015). *National strategic assessment of serious and organised crime 2015*. Retrieved from the National Crime Agency website: http://www.nationalcrimeagency.gov.uk/publications/560-national-strategic-assessment-of-serious-and-organised-crime-2015/file

National Crime Agency. (2016). *National Crime Agency annual report and accounts 2015-16*. Retrieved from the National Crime Agency website: http://www.nationalcrimeagency.gov.uk/publications/715-national-crime-agency-annual-report-and-accounts-2015-16/file

National Criminal Intelligence Service. (2000). *The national intelligence model*. Retrieved from the Intelligence Analysis website: http://www.intelligenceanalysis.net/National%20Intelligence%20Model.pdf

National Economic Research Associates. (2007). *The economic cost of fraud*. Retrieved from the National Economic Research Associates website: http://www.nera.com/image/3779.pdf

National Fraud Authority. (2010a). *Information sharing project: report on data sharing for the prevention of fraud under section 68 of the Serious Crime Act 2007*. Retrieved from Home Office, National Fraud Authority website: http://www.homeoffice.gov.uk/publications/agencies-public-bodies/nfa/our-work/info-sharing-serious-crime-act?view=Binary

National Fraud Authority. (2010b). *Information sharing report: progress update.* Retrieved from Home Office, National Fraud Authority website: http://www.homeoffice.gov.uk/publications/agencies-public-bodies/nfa/our-work/info-sharing-progress-update?view=Binary

National Fraud Authority. (2011a). *Business plan 2011/12*. Retrieved from Home Office, National Fraud Authority website: http://www.homeoffice.gov.uk/publications/agencies-public-bodies/nfa/business-plans/business-plan-2011-12?view=Binary

National Fraud Authority. (2011b). *Fighting fraud together: the strategic plan to reduce fraud*. Retrieved from the Home Office, National Fraud Authority website: http://www.homeoffice.gov.uk/publications/agencies-public-bodies/nfa/fighting-fraud-tog/fighting-fraud-together?view=Binary

National Fraud Authority. (2012). *Annual Fraud Indicator March 2012.* Retrieved from the National Fraud Authority website: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/118530/annual-fraud-indicator-2012.pdf

National Fraud Authority. (2013). *Annual fraud indicator June 2013*. Retrieved from the National Fraud Authority website: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/206552/nfa-annual-fraud-indicator-2013.pdf

National Fraud Strategic Authority. (2009). *The national fraud strategy: a new approach to combating fraud*. Retrieved from the National Fraud Authority website: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/118480/national-fraud-strategy.pdf

Noaks, L. & Wincup. E. (2004). *Criminological research: understanding qualitative methods*. London: SAGE.

Noor, K.B.M. (2008). Case study: a strategic research methodology. *American Journal of Applied Sciences 5*(11), 1602-1604. doi: 10.3844/ajassp.2008.1602.1604

Noordegraaf, M. (2007). From “pure” to “hybrid” professionalism: present day professionalism in ambiguous public domains. *Administration & Society, 39*(6), 761-785. doi: 10.1177/0095399707304434

O’Leary, Z. (2007). *The social science jargon-buster: the key terms you need to know*. London: SAGE.

O’Regan, D. (2001). Genesis of a profession: towards professional status for internal auditing. *Managerial Auditing Journal, 16*(4), 215-226. doi: 10.1108/02686900110389160

Office for National Statistics. (2016). *Crime in England and Wales year ending Mar 2016*. Retrieved from the Office for National Statistics website: http://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmar2016

Oppel Jr., R.A. & Sorkin, A.R. (2001, November 29). Enron's collapse: the overview; Enron collapses as suitor cancels plans for merger. *The New York Times*. Retrieved from http://www.nytimes.com/2001/11/29/business/enron-s-collapse-the-overview-enron-collapses-as-suitor-cancels-plans-for-merger.html?pagewanted=all&_r=0

Organisation for Economic Co-operation and Development. (2008). *The economic impact of counterfeiting and piracy*. Retrieved from the Organisation for Economic Co-operation and Development website: http://www.keepeek.com/Digital-Asset-Management/oecd/trade/the-economic-impact-of-counterfeiting-and-piracy_9789264045521-en#page1

Oswald, M. (2013). Joining the dots - intelligence and proportionality. *Privacy & Data Protection, 13*(5), 6-8. Retrieved from the University of Winchester website: http://www.winchester.ac.uk/academicdepartments/Law/Centre%20for%20Information%20Rights/Publications/Documents/Joining%20the%20dots%20-%20intelligence%20and%20proportionality%20-%20Marion%20Oswald.pdf

Otjacques, B., Hitzelberger, P. & Feltz, F. (2007). Interoperability of e-government information systems: issues of identification and data sharing. *Journal of Management Information Systems, 23*(4), 29-51. doi: 10.2753/MIS0742-1222230403

Pardo, T.A., Cresswell, A.M., Dawes, S.S. & Burke, G.B. (2004). Modeling the social and technical processes of interorganizational information integration. *Proceedings of the 37th Hawaii International Conference on System Sciences*. Retrieved from http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1265307

Pardo, T.A., Cresswell, A.M., Thompson, F. & Zhang, J. (2006). Knowledge sharing in cross-boundary information system development in the public sector. *Information Technology and Management, 7*(4), 293-313. doi: 10.1007/s10799-006-0278-6

Pardo, T.A., Gil-Garcia, J.R. & Burke, G.B. (2006). *Building response capacity through cross-boundary information sharing: the critical role of trust*. Retrieved from http://dev5.ctg.albany.edu/publications/journals/e-2006_building_response/e-2006_building_response.pdf

Pardo, T.A., Gil-Garcia, J.R. & Burke, G.B. (2008). Governance structures in cross-boundary information sharing: lessons from state and local criminal justice initiatives. *Proceedings of the 41st Hawaii International Conference on System Sciences*. Retrieved from http://dl.acm.org/citation.cfm?id=1334866

Pardo, T.A. & Tayi, G.K. (2007). Interorganizational information integration: a key enabler for digital government. *Government Information Quarterly, 24*(4), 691-715. doi: 10.1016/j.giq.2007.08.004

Pavlin, S., Svetlik, I. & Evetts, J. (2010). Revisiting the role of formal and practical knowledge from a sociology of the professions perspective: the case of Slovenia. *Current Sociology, 58*(1), 94-118. doi: 10.1177/0011392109348547

Performance and Innovation Unit. (2002). *Privacy and data-sharing: the way forward for public services*. Retrieved from the National Archives website: http://webarchive.nationalarchives.gov.uk/+/http://www.cabinetoffice.gov.uk/upload/assets/www.cabinetoffice.gov.uk/strategy/piu-data.pdf

Phythian, M. (2013). Introduction: beyond the intelligence cycle? In M. Phythian (Ed.), *Understanding the intelligence cycle* (pp.1-8). Abingdon: Routledge.

Police ICT. (n.d.). *National Intelligence Model standard.* Retrieved from the Police ICT website: https://ict.police.uk/national-standards/intel/

Powell, W.W. (1990). Neither market nor hierarchy: network forms of organization. In B.M. Staw & L.L. Cummings (Eds.), *Research in organizational behaviour volume 12* (pp.295-336). Retrieved from https://www.researchgate.net/profile/Walter_Powell/publication/31842399_Neither_Market_nor_Hierarchy_Network_Forms_of_Organization_WW_Powell/links/0f317533c8be2c9568000000.pdf

PwC. (2016). *Global economic crime survey 2016: adjusting the lens on economic crime*. Retrieved from the PwC website: http://www.pwc.com/gx/en/economic-crime-survey/pdf/GlobalEconomicCrimeSurvey2016.pdf

Ratcliffe, J. (2002). Intelligence-led policing and the problems of turning rhetoric into practice. *Policing and Society: An International Journal of Research and Policy, 12*(1), 53-66. doi: 10.1080/10439460290006673

Robson, C. (2011). *Real world research: a resource for users of social research methods in applied settings* (3rd ed.). Chichester: John Wiley & Sons.

Rowley, J. (2006). The wisdom hierarchy: representations of the DIKW hierarchy. *Journal of Information Science, 33*(2), 163-180. doi: 10.1177/0165551506070706

Saldaña, J. (2013). *The coding manual for qualitative researchers* (2nd ed.). London: SAGE.

Sale, J.E.M., Lohfeld, L.H. & Brazil, K. (2002). Revisiting the quantitative-qualitative debate: implications for mixed-methods research. *Quality & Quantity, 36*(1), 43-53. doi: 10.1023/A:1014301607592

Sampson, H. (2004). Navigating the waves: the usefulness of a pilot in qualitative research. *Qualitative Research, 4*(3), 383-402. doi: 10.1177/1468794104047236

Sarathy, R. & Muralidhar, K. (2006). Secure and useful data sharing. *Decision Support Systems, 42*(1), 204-220. doi: 10.1016/j.dss.2004.10.013

Sawyer, R. D. (1998). *The tao of spycraft: intelligence theory and practice in traditional China*. Boulder: Westview.

Schein, E.H. (1996). Culture: the missing concept in organization studies. *Administrative Science Quarterly, 41*(2), 229-240. doi: 10.2307/2393715

Schein, E.H. (2009). *The corporate culture survival guide: new and revised edition*. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.465.7545&rep=rep1&type=pdf

Schooley, B.L. & Horan, T.A. (2007). Towards end-to-end government performance management: case study of interorganizational information integration in emergency medical services (EMS). *Government Information Quarterly, 24*(4), 755-784. doi: 10.1016/j.giq.2007.04.001

Semmens, N. (2011). Methodological approaches to criminological research. In P. Davies, P. Francis & V. Jupp (Eds.), *Doing criminological research* (2nd ed.) (pp.54-77). London: SAGE.

Sheptycki, J. (2004). Organizational pathologies in police intelligence systems: some contributions to the lexicon of intelligence-led policing. *European Journal of Criminology, 1*(3), 307-332. doi: 10.1177/1477370804044005

Smith, G., Button, M., Johnston, L. & Frimpong, K. (2011). *Studying fraud as white collar crime*. Basingstoke: Palgrave Macmillan.

Smith, K., Seligman, L. & Swarup, V. (2008). Everybody share: the challenge of data-sharing systems. *Computer, 41*(9), 54-61. Retrieved from http://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=2

Soanes, C. & Stevenson, A. (Eds.). (2006). *Concise Oxford English dictionary* (11th ed., revised edition). Oxford: Oxford University Press.

Stake, R.E. (1978). The case study method in social inquiry. *Educational Researcher, 7*(2), 5-8. Retrieved from http://www.jstor.org/journal/educrese

Strachan-Morris, D. (2013). The intelligence cycle in the corporate world: bespoke or off-the-shelf? In M. Phythian (Ed.), *Understanding the intelligence cycle* (pp.119-133). Abingdon: Routledge.

Syed-Ikhsan, S.O.S. & Rowland, F. (2004). Knowledge management in a public organization: a study on the relationship between organizational elements and the performance of knowledge transfer. *Journal of Knowledge Management, 8*(2), 95-111. doi: 10.1108/13673270410529145

Thomas, G. (2011). *How to do your case study: a guide for students & researchers*. London: SAGE.

Thomas, R. & Walport, M. (2008). *Data sharing review report*. Retrieved from the NHS Connecting for Health website: http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/links/datasharingreview.pdf

Tilley, N. (2003). Community policing, problem-oriented policing and intelligence-led policing. In T. Newburn (Ed.), *Handbook of policing* (pp.311-339). Retrieved from http://lib.myilibrary.com/Open.aspx?id=133171

Trafford, V. & Leshem, S. (2008). *Stepping stones to achieving your doctorate: focusing on your viva from the start*. Maidenhead: Open University Press.

Tzu, S. (1971). *The art of war* (S.B. Griffith, Trans.). Oxford: Oxford University Press. (Original work published c.490 B.C.)

UK Fraud Costs Measurement Committee. (2016). *Annual fraud indicator 2016*. Retrieved from the University of Portsmouth website: http://www.port.ac.uk/media/contacts-and-departments/icjs/ccfs/Annual-Fraud-Indicator-2016.pdf

University of Portsmouth. (n.d.). *Centre for Counter Fraud Studies: Counter Fraud Professional Accreditation Board*. Retrieved from http://www.port.ac.uk/centre-for-counter-fraud-studies/counter-fraud-professional-accreditation-board/

University of Portsmouth. (2015). Ethics policy. Retrieved from http://policies.docstore.port.ac.uk/policy-028.pdf

U.S. Securities and Exchange Commission Office of Investigations. (2007). *Investigation of failure of the SEC to uncover Bernard Madoff's Ponzi scheme - public version*. Retrieved from the SEC website: https://www.sec.gov/news/studies/2009/oig-509.pdf

van Teijlingen, E.R. & Hundley, V. (2001). The importance of pilot studies. *Social Research Update, 35*, 1-4. Retrieved from http://sru.soc.surrey.ac.uk/

van Wijk, R., Jansen, J.J.P. & Lyles, M.A. (2008). Inter- and intra-organizational knowledge transfer: a meta-analytic review and assessment of its antecedents and consequences. *Journal of Management Studies, 45*(4), 830-853. doi: 10.1111/j.1467-6486.2008.00771.x

Wakefield, A. (2011). Undertaking a criminological literature review. In P. Davies, P. Francis & V. Jupp (Eds.), *Doing criminological research* (2nd ed.) (pp.78-98). London: SAGE.

Warner, M. (2002). Wanted : a definition of intelligence. *Studies in Intelligence, 46*(3), 15-22. Retrieved from https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies

Warner, M. (2013). The past and future of the intelligence cycle. In M. Phythian (Ed.), *Understanding the intelligence cycle* (pp.9-20). Abingdon: Routledge.

Wendel, W.B. (2001). Morality, motivation, and the professional movement. *South Carolina Law Review, 52*(3), 557-608. Retrieved from https://litigation-essentials.lexisnexis.com/webcd/app?action=DocumentDisplay&crawlid=1&srctype=smi&srcid=3B15&doctype=cite&docid=52+S.C.+L.+Rev.+557&key=238eebc5ac453cb0ad019c6235c480d2

Wenjing, L. (2011). Government information sharing: principles, practice, and problems – an international perspective. *Government Information Quarterly, 28*(3), 363-373. doi: 10.1016/j.giq.2010.10.003

Wheaton, K.J. & Beerbower, M.T. (2006). Towards a new definition of intelligence. *Stanford Law & Policy Review, 17*(2), 319-330. Retrieved from https://journals.law.stanford.edu/stanford-law-policy-review

Whelan, C. (2015, March 19). Security networks and occupational culture: understanding culture within and between organisations. *Policing and Society*. Retrieved from http://www.tandfonline.com/doi/pdf/10.1080/10439463.2015.1020804?needAccess=true

Willem, A. & Buelens, M. (2007). Knowledge sharing in public sector organizations: the effect of organizational characteristics on interdepartmental knowledge sharing. *Journal of Public Administration Research and Theory, 17*(4), 581-606. doi: 10.1093/jopart/mul021

Williams, C.B., Dias, M., Fedorowicz, J., Jacobson, D., Vilvovsky, S., Sawyer, S. & Tyworth, M. (2009). The formation of inter-organizational information sharing networks in public safety: cartographic insights on rational choice and institutional explanations. *Information Polity, 14*(1-2), 13-29. doi: 10.3233/IP-2009-0170

Yang, T-M. & Maxwell, T.A. (2011). Information-sharing in public organizations: a literature review of interpersonal, intra-organizational and inter-organizational success factors. *Government Information Quarterly, 28*(2), 164-175. doi: 10.1016/j.giq.2010.06.008

Yang, T-M., Zheng, L. & Pardo, T. (2012). The boundaries of information sharing and integration: a case study of Taiwan e-government. *Government Information Quarterly, 29*(Supplement 1), S51-S60. doi: 10.1016/j.giq.2011.08.014

Yin, R.K. (2006). Mixed methods research: are the methods genuinely integrated or merely parallel? *Research in the Schools, 13*(1), 41-47. Retrieved from http://connection.ebscohost.com/

Yin, R.K. (2009). *Case study research: design and methods (4th ed.)*. London: SAGE.

Yin, R.K. (2012). *Applications of case study research* (3rd ed.). Thousand Oaks: SAGE.

Yiu, C. (2012). *The big data opportunity: making government faster, smarter and more personal*. London: Policy Exchange. Retrieved from http://www.policyexchange.org.uk/images/publications/the%20big%20data%20opportunity.pdf

Zeng, D., Chen, H., Daspit, D., Shan, F., Nandiraju, S., Chau, M. & Lin, C. (2003). COPLINK Agent: an architecture for information monitoring and sharing in law enforcement. *Intelligence and Security Informatics, 2665*, 281-295. doi: 10.1007/3-540-44853-5_21

Zhao, J.L., Bi, H.H., Chen, H., Zeng, D.D., Lin, C. & Chau, M. (2004). Process-driven collaboration support for intra-agency crime analysis. *Decision Support Systems, 41*(3), 616-633. doi: 10.1016/j.dss.2004.06.014

Zhang, J. & Dawes, S.S. (2006). Expectations and perceptions of benefits, barriers, and success in public sector knowledge networks. *Public Performance and Management Review, 29*(4), 433-466. Retrieved from http://www.jstor.org/stable/20447606

Zhang, J., Dawes, S.S. & Sarkis, J. (2005). Exploring stakeholders' expectations of the benefits and barriers of e-government knowledge sharing. *The Journal of Enterprise Information Management, 18*(5), 548-567.

Zheng, L., Dawes, S. & Pardo, T.A. (2009). Leadership behaviours in cross-boundary information sharing and integration: comparing the US and China. Proceedings of the 3rd International Conference on Theory and Practice of Electronic Governance. Retrieved from http://dl.acm.org/citation.cfm?id=1693042.1693052

Zheng, L., Jiang, Y., Yang, T-M. & Pardo, T. (2008). Sharing information for product quality and food safety in China: barriers and enablers. *Proceedings of the 2nd International Conference on Theory and Practice of Electronic Governance.* Retrieved from http://dl.acm.org/citation.cfm?id=1509096&picked=prox&CFID=356079964&CFTOKEN=46098262

Zheng, L., Yang, T-M., Pardo, T. & Jiang, Y. (2009). Understanding the "boundary" in information sharing and integration. *Proceedings of the 42nd Hawaii International Conference on System Sciences*. Retrieved from http://dl.acm.org/citation.cfm?id=1490119&CFID=248253384&CFTOKEN=61394894

Appendices

Appendix One: Ethics Risk Assessment

ICJS Ethics Self-Assessment Form

Introduction

All research involving human participants, animals and/or sensitive data undertaken by students and staff *must* receive a **favourable ethical opinion** before it can be undertaken and, if appropriate, subsequently used for publication.

The completion of this **ICJS Ethics Self-Assessment Form** is the **start point** for applying for favourable ethical opinion and as such it is a record of the ethical considerations that have been addressed in planning the research proposal.

The ICJS Ethics Self-Assessment **Form** has **4 sections**, **all of which must be completed.**

Section 1: Student details and proposed research topic

Section 2: Preparation; and details of ethical issues identified in the proposed research

Section 3: Ethical Narrative

Section 4: Ethical Opinion Outcome Record

A copy of this completed Self-Assessment Form should be supplied with your research proposal. It will then be passed on to your dissertation supervisor.

You may not proceed to data collection until you have received a favourable ethical opinion.

Please see the document: **'How to Apply for Ethical Review'** for the process that you will need to follow in order to receive a favourable ethical opinion.

Section 1: Student details and proposed research topic

Student name: .Carl Watson ……

Student number:…441864……

Proposed research topic:

...Information and Intelligence Sharing in the Fight Against Fraud ……

……

Section 2: Preparation and details of ethical issues identified in the proposed research

1. Student has read the *British Society of Criminology* ethical guidelines.
www.britsoccrim.org/codeofethics.htm Yes [x] **No [ ]**

2. Student has participated in research ethics sessions (lecture/seminar/workshop/other on-line or face to face activity) provided by their programme of study.
Yes [x] **No [ ]**

3. Will the research involve the collection and analysis of primary or secondary data?

Primary data	Yes [x]	No [ ]
Secondary data	Yes [ ]	No [x]

Note: Secondary data is data that has already been collected by other researchers or an organisation for another purpose. Data may be in the public domain or available under the Freedom of Information Act (2000).

If 'No' to both parts of Q3, go to Q16.

If 'Yes' to both or either parts of Q3, go on to answer ALL of the questions on the following pages.

4. Does proposed research involve face-to-face contact with members of the community (including professionals and those held or 'looked after')?

Yes [x] No [ ]

5. Is access to personal or confidential data sought? **Yes [ ]** No [x]

Note 1: This question applies to both primary and secondary data.

Note 2: You should be aware that privileged access to contact details or information as a result of a professional role, links to a host organization or personal association is considered to be ethically problematic and arrangements should be made for third party anonymised access.

6. Are you aware of the need to ensure anonymity and confidentiality of research participants?

Yes [x] **No [ ]**

7. Are there potential risks (to you and/or research subjects) in the research? (If 'Yes', then specify these risks in the spaces provided.)

Physical risks – to participants **Yes [ ]** No [x]

……

……

Physical risks – to yourself **Yes [ ]** No [x]

……

……

Psychological risks – to participants **Yes [ ]** No [x]

……

……

Psychological risks – to yourself **Yes [ ]** No [x]

……

……

Compromising situations – to participants **Yes [ ]** No [x]

……

……

Compromising situations – to yourself **Yes [ ]** No [x]

……

……

8. Do you believe you need to deceive research subjects? (e.g. by not being clear about the purpose of your research)

Yes [ ] No [x]

9. Is there any likely harm to participants involved in the research?

Yes [ ] No [x]

10. Is participation in the research entirely voluntary? Yes [x] **No [ ]**

11. Have you considered how you are going to obtain informed consent from research participants?

Yes [x] **No [ ]**

12. Is there any potential role conflict for you in the research? **Yes [ ]** No [x]

Note: Role conflict is defined as any contact with a participant who knows you (the researcher) in another capacity. Commonly this is a professional capacity.

13. If you are using secondary data, is the data available in the public domain?

Yes [ ] **No** [ ] Not using secondary data [x]

If "No", please explain:

- how you have access to the data .....
- the arrangements you have made with the host organisation/holder of the information to receive the data in an anonymised state which conforms to the Data Protection Act (1998)

  .....
  .....
  .....

14. If access to data outside of the public domain is proposed, have you consulted with your data protection officer?

Yes [ ] **No** [x]

15. Are there any other data protection issues? **Yes [ ]** No [X]

16. Are there *any other* potential sources of ethical issues or conflict in the proposed research (e.g. political considerations, sensitivity of the topic, reputational issues for researcher, participants and/or host organisation)?

Yes [x] No [ ]

If 'Yes', then specify these risks ……..

As part of the research is to involve case study research into organizations, there are inherent reputational risks relevant to the participating organization, as this type of research will involve the organization and information about the organization relevant to the research, being identified in the thesis and any subsequent publications arising from the research. Furthermore, there is a risk that the researcher may be exposed to potentially sensitive data during the data collection phase of the case study research.

I confirm that:

- the information provided is a complete and accurate record of my plans at present;
- I have read and understood the process for obtaining a favourable ethical opinion as contained in the document: 'How to Apply for Ethical Review'; and
- I shall resubmit an amended version of this form should my research alter significantly such that there is any significant variation of ethical risk.

Signed: …Carl Watson…….. Student

Signed: …… …… Dissertation/research supervisor

Date: ……11-11-2013……

Advice/ decisions/ responsibilities

Answers in bold and underlined require further consideration as they pose potential ethical issues.

If any of the questions you have require further consideration, you must:

- attach additional details in an Ethical Narrative (see following page) of how you plan to minimize any risks identified; and
- discuss these issues with your dissertation/research supervisor/tutor

Once your dissertation/research supervisor/tutor has agreed that you are ready to apply for ethical review, you must follow the process for obtaining a favourable ethical opinion as contained in the document: 'How to Apply for Ethical Review'. **You may not proceed to data collection until favourable ethical opinion** has been given by the ICJS Ethics Committee or the Faculty Ethics Committee (FEthC) (as appropriate).

Your dissertation/research supervisor/tutor has the responsibility for ethical oversight of your research. You must keep them informed of any changes to your proposed research. Your supervisor in turn may wish to consult with the ICJS Ethics Adviser and/or the ICJS Ethics Committee if they have concerns about the ethical implications of any aspect of your research strategy. Jane Winstone is the ICJS Ethics Adviser and Ethics Lead for the ICJS Ethics Committee (icjsethics@port.ac.uk)

Section 3: Ethical Narrative

There are a number of ethical issues that have to be addressed with respect to this research, and the methods to be employed within the study. The research topic itself – information and intelligence sharing – is not in itself a sensitive issue, and so there are no immediate ethical issues that are perceived to arise with regards to the immediate subject matter. Rather, the issues that do need to be addressed arise due to the nature of the methods (qualitative interviews and case study research) to be employed, as these will require the collection of primary data involving interaction with members of the community, and the participation of an organisation, or organisations, as the subject of a case study.

The research study will involve face-to-face contact with members of the community – specifically people with professional knowledge and understanding of anti-fraud and law-enforcement related information and intelligence sharing issues – as the intended research methods involve quantitative research interviews and case study research. Participants in these data gathering exercises will be protected from adverse risk by way of the following steps, which will be implemented in order to observe both a level of fundamental respect for

participants (Macfarlane, 2009, p.9), and wider societal values and the cultural context of research ethics (Brinkmann & Kvale, 2005, p.162; Denscombe, 2010, pp.59-60).

Firstly, in line with the principle of *informed consent (*British Society of Criminology, 2006, p.3; Davies, 2011, p.167; Davies & Francis, 2011, pp.283-284), research participants will be fully informed about the nature and aims of the study, and of the implications of their involvement (including anticipated output and outcomes, and possible publication of the research findings) in order that they can make a reasoned and informed judgement about whether or not they wish to take part. All efforts will be made to ensure that this consent is voluntary (Macfarlane, 2009, p.3), and it will be made clear to prospective participants that the decision is entirely theirs whether or not they wish to join the study. This will be set out in both invitation letters and information sheets to be issued to prospective candidates. It is recognised that this issue may be more straightforward for those persons invited to take part in a stand-alone research interview than for employees of the organisation(s) that takes part in the case study research. In respect of the latter, the invitation letters and information sheets make it clear that, while the organisation has consented to take part in the research, this in no way places any obligation on them to do the same, and again inform them that the decision of whether or not to take part is their own.

Participants will be informed of their right to withdraw – which will be possible up to the stage of analysis and integration of the data with the wider data, and will be advised how to do so in the information sheet. They shall also be reminded about this immediately prior to their involvement (for example, at the commencement of an interview). Participants will not be deceived about any aspect of the research, and the nature and purpose of it will be made clear to them during any access negotiation, and set out in the research information sheets that they will receive copies of.

Interviews conducted, and any other forms of participation (such as observation sessions / job shadowing) during the case study element of the research, will be entirely anonymous with neither the identity of the individual nor that of their employing organisation being disclosed in the thesis or any subsequently published output from the research. The sole anticipated exception to the notion of organisational anonymity will, necessarily, be that of the subject of the case study – the Federation Against Copyright Theft (FACT). The issue of the need to identify FACT within the output of the research has been discussed with that organisation during access negotiation. As part of this, the organisation has been reassured that while the organisation name will be reported, none of the officers or staff will be identified in the output. However, it has been pointed out within the

information sheet that there are risks that some individuals' identities may be inferred where they are known to work for this organisation. These risks will be mitigated insofar as is possible through careful reporting of the findings of the case study, but it has been necessary to inform the organisation, and individual participants, that a residual risk remains in this respect.

Participants' data will be kept securely and in line with the requirements of the Data Protection Act 1998, and will be kept and used solely in line with the purposes for which it was collected. It will not be shared with others, and it will be kept for no longer than is necessary for the purposes of the research and in line with the requirements and guidelines of the University of Portsmouth and the requirements of the Professional Doctorate programme examiners – I propose that the primary data collected shall be securely destroyed within a month of the degree being awarded (or my permanently leaving the programme if it is not successfully completed). Data collected shall be transferred as quickly as possible after the interviews from the audio recording device to a password protected laptop to which I have sole access. A back up of the data will be stored on an encrypted external hard drive, again to which only I have access. The information sheets to be issued to prospective participants contain details with respect to these data handling issues, including with respect to the storing and ultimate destruction of the data. Furthermore, it makes clear the possibility that the data may be reviewed by certain parties involved in the doctoral research process, such as the research supervisor, examiners and, potentially, auditors.

Reporting of data, including within the thesis and any interim or subsequent publication and dissemination of the findings, will be reviewed in order to ensure that participants' identities are not discernible from the output. Where reference may need to be made to an individual's responses, such as in a quotation or excerpt from an interview, a generic reference tag shall be assigned (such as *Interviewee #1*).

Where interview-based and other data is collected using an audio recording device, participants will be asked for their consent for this method to be used. This is again outlined in the information sheets to be provided to potential participants. If they do not give such express consent, an audio recording device will not be used in that part of the research. Where participants do so consent, they will be reminded of this at the start of the interview or other research situation.

Implications and potential risks have been discussed with the case study organisation, and they have been made aware of the proposed methods and implications of them (such as the researcher being on site for a period of time as an observer conducting embedded case study research). The organisation is fully

aware that this will involve the researcher spending time at their facilities and with employees. As such, and as the organisation is involved in the investigation of crime, there is the risk that the researcher may be exposed to information of a sensitive nature about its operations, investigations and possibly suspects or witnesses. This was discussed during access negotiation, and has been addressed within the information sheet, with assurances given that such information will not be reported, and through providing an undertaking to sign any relevant confidentiality agreements in respect of such information.

As noted above the organisation has been made fully aware that, as a research case study, it will be necessary to name it within the thesis, and possible further output for publication, and has been made aware that there is a risk of reputational impact in respect of this. While the case study will be handled, and reported, sensitively, this risk is outside of the full control of the researcher, and so it is necessary and fair to notify the organisation of this.

Other than the risks identified above, there are no perceived additional risks that are likely to arise from the research for the participants or the researcher. Furthermore, there is no perceived issue relating to potential role conflict within the research. The research – both the stand-alone qualitative research interviews and the case study element – is being conducted outside of my own organisation, and with organisations and people that I have no formal relationship with. Neither, to the fullest extent of my knowledge, does my employing organisation have any formal link with any of the people or organisations that I aim to include within the research. As such, this minimises the potential for role conflict or any perceived obligation on the part of any potential research participant to join the study.

It is made clear within the research information sheets for potential participants that the research is not being funded by way of a research grant, and is being conducted for the purposes of the Professional Doctorate course at the University of Portsmouth. As such, the research data will be owned by the University of Portsmouth. In line with the fifth data protection principle (Information Commissioner's Office, 2001, p.26), the primary research data will not be kept longer than is necessary than for the purpose of the doctoral programme, and the information sheets provide assurances to potential participants that it will be destroyed after completion of the degree.

References

Brinkmann, S. & Kvale, S. (2005). Confronting the ethics of qualitative research. *Journal of Constructivist Psychology, 18*(2), 157-181. doi: 10.1080/10720530590914789

British Society of Criminology. (2006). *Code of ethics for researchers in the field of criminology*. Retrieved from: http://www.britsoccrim.org/docs/CodeofEthics.pdf

Davies, P. (2011). Doing interviews in prison. In P. Davies, P. Francis & V. Jupp (Eds.), *Doing criminological research* (2nd ed.) (pp.161-178). London: SAGE.

Davies, P. & Francis, P. (2011). Reflecting on criminological research. In P. Davies, P. Francis & V. Jupp (Eds.), *Doing criminological research* (2nd ed.) (pp.281-285). London: SAGE.

Denscombe, M. (2010). *Ground rules for social research: guidelines for good practice* (2nd ed.). Maidenhead: Open University Press.

Information Commissioner's Office. (2001). *The data protection act 1998: legal guidance*. Wilmslow: Information Commissioner's Office.

Macfarlane, B. (2009). *Researching with integrity: what does it really mean to be an ethical researcher?* Retrieved from University of Portsmouth, Victory Research Methods Hub website: https://victory.port.ac.uk/webct/urw/lc5116011.tp0/cobaltMainFrame.dowebct

Section 4: Ethical Opinion Outcome Record

This section will be completed by the ICJS Ethics Committee for: Undergraduate, Masters and DCrimJ (Professional Doctorate) [Stage 2,1, ART] research proposals and therefore this document **must be included in the Ethical Bundle when it is sent for ethical review to Jane Winstone (icjsethics@port.ac.uk)**

A copy of the outcome of ethical opinion will be sent to the student who is responsible for providing this to the dissertation/research supervisor. A copy will also be kept on record by the ICJS Ethics Committee.

Please note: PhD candidates will be notified of a favourable ethical opinion in a letter from the Faculty Ethics Committee (FEthC) which will include a REC number. (For further details of this see the document: 'How to Apply for Ethical Opinion' – Stage 2: The process for applying for ethical opinion.)

ICJS EC Ethical Opinion Outcome Record*	
Favourable ethical opinion You can commence data collection with the agreement of your supervisor.	
Provisional favourable ethical opinion subject to requirements. **See 'Comments' on following page.** Once your supervisor is satisfied that you have met these requirements, you may commence data collection.	
RISKS ASSESSED AS SIGNIFICANT and a favourable ethical opinion cannot be provided for the proposal in its present form. **See 'Comments' on following page.** You must revise your proposal in consultation with your supervisor. Once your supervisor is satisfied that you have addressed all of the Comments below, you may resubmit for ethical opinion You may not commence data collection.	

*The ICJS EC default position is to reserve the right to refer any research proposal to the Faculty Ethics Committee where the proposal poses ethical issues beyond its remit to form an opinion upon.

Date complete ethical bundle received fit for review: ……

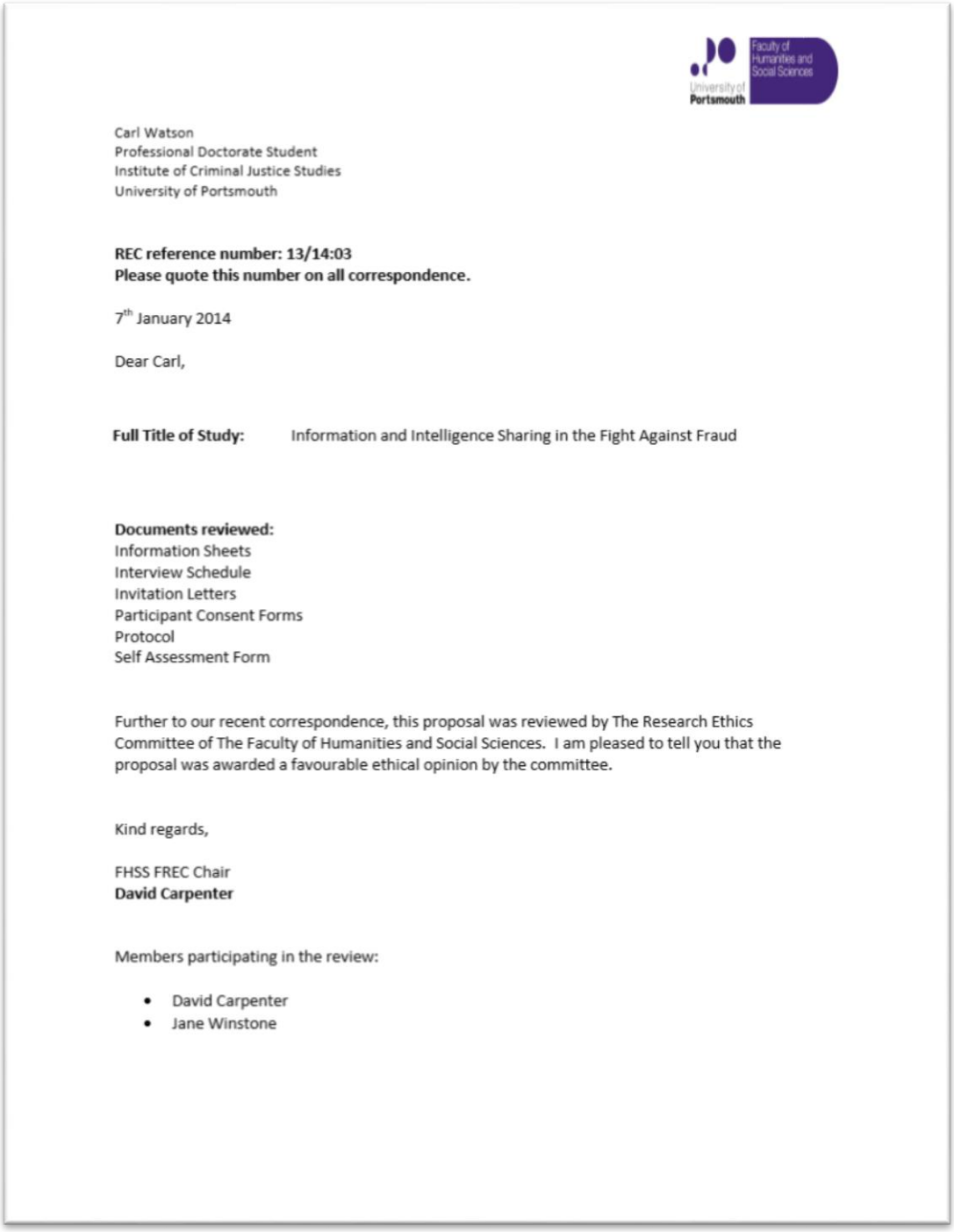
Date reviewed: ……

Signed: …… (Member of ICJS Ethics Committee)

Section 4 (continued):

Comments to Support Ethical Opinion Outcome Record

Appendix Two: Ethical Approval Letter



Faculty of Humanities and Social Sciences
University of Portsmouth

Carl Watson
Professional Doctorate Student
Institute of Criminal Justice Studies
University of Portsmouth

REC reference number: 13/14:03
Please quote this number on all correspondence.

7th January 2014

Dear Carl,

Full Title of Study: Information and Intelligence Sharing in the Fight Against Fraud

Documents reviewed:
Information Sheets
Interview Schedule
Invitation Letters
Participant Consent Forms
Protocol
Self Assessment Form

Further to our recent correspondence, this proposal was reviewed by The Research Ethics Committee of The Faculty of Humanities and Social Sciences. I am pleased to tell you that the proposal was awarded a favourable ethical opinion by the committee.

Kind regards,

FHSS FREC Chair
David Carpenter

Members participating in the review:

- David Carpenter
- Jane Winstone

Appendix Three: Research Ethics Review Checklist

FORM UPR16

Research Ethics Review Checklist

University of Portsmouth

Please include this completed form as an appendix to your thesis (see the Postgraduate Research Student Handbook for more information

Postgraduate Research Student (PGRS) Information			Student ID:	441864
PGRS Name:	Carl Watson			
Department:	Institute of Criminal Justice Studies	First Supervisor:	Professor Mark Button	
Start Date: (or progression date for Prof Doc students)	01 October 2013			
Study Mode and Route:	Part-time ☒ Full-time ☐	MPhil ☐ PhD ☐	MD ☐ Professional Doctorate ☒	

Title of Thesis:	Information and Intelligence Sharing in the Fight Against Fraud and Intellectual Property Crime: Challenges and Strategies for Professional Practice
Thesis Word Count: (excluding ancillary data)	48,663

If you are unsure about any of the following, please contact the local representative on your Faculty Ethics Committee for advice. Please note that it is your responsibility to follow the University's Ethics Policy and any relevant University, academic or professional guidelines in the conduct of your study

Although the Ethics Committee may have given your study a favourable opinion, the final responsibility for the ethical conduct of this work lies with the researcher(s).

UKRIO Finished Research Checklist:
(If you would like to know more about the checklist, please see your Faculty or Departmental Ethics Committee rep or see the online version of the full checklist at: http://www.ukrio.org/what-we-do/code-of-practice-for-research/)

a) Have all of your research and findings been reported accurately, honestly and within a reasonable time frame?	YES ☒ NO ☐
b) Have all contributions to knowledge been acknowledged?	YES ☒ NO ☐
c) Have you complied with all agreements relating to intellectual property, publication and authorship?	YES ☒ NO ☐
d) Has your research data been retained in a secure and accessible form and will it remain so for the required duration?	YES ☒ NO ☐
e) Does your research comply with all legal, ethical, and contractual requirements?	YES ☒ NO ☐

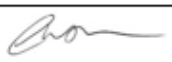
Candidate Statement:

I have considered the ethical dimensions of the above named research project, and have successfully obtained the necessary ethical approval(s)

Ethical review number(s) from Faculty Ethics Committee (or from NRES/SCREC):	13/14:03

If you have *not* submitted your work for ethical review, and/or you have answered 'No' to one or more of questions a) to e), please explain below why this is so:

UPR16 – August 2015

Signed *(PGRS)*:		Date: 16 April 2017

Appendix Four: Phase Two Interviews Invitation Letter

Study Title: ..Information and Intelligence Sharing in the Fight Against Fraud

FHSS REC Ref No: .....

Dear Potential Participant

I would like to invite you to participate in a research study into Information and Intelligence Sharing in the Fight Against Fraud.

I am a postgraduate research student at the Institute of Criminal Justice Studies at the University of Portsmouth, taking a Professional Doctorate in Criminal Justice course. For this degree course, I am conducting research into anti-fraud information and intelligence sharing, with a view to increasing understanding of inter-organisational collaboration and how to overcome the challenges that impede it.

I have obtained your details from [Insert] and think that you would be a suitable participant in this study given your position within [organisation name]. I am inviting you to take part in a qualitative research interview into information and intelligence sharing.

I have enclosed with this letter a Participant Information Sheet containing further details of the research. If you are willing to take part in the study, I would request that you confirm that you are willing to do so, and I have provided my contact details below. Prior to the commencement of the case study research, I will ask you to complete and sign a Consent Form, a copy of which is enclosed for your information. I will bring copies of this to be signed prior to the interview taking place.

My contact details are:

Carl Watson
[redacted]

Email: carl.watson@myport.ac.uk

Mobile: [redacted]

Participation in the research is entirely voluntary. If you give consent to take part in a research interview, but subsequently change your mind, you may withdraw from the interview before, during or immediately after the interview has taken place. However, it may not be possible to withdraw once the research has been completed and the data analysed and integrated with the rest of the research data. If you do wish to withdraw, please inform the researcher using the contact details above.

Date: Version No. CW/RI/1

Thank you for reading this letter, regardless of whether or not you choose to take part in the study.

Yours sincerely

Carl Watson
Postgraduate Research Student
University of Portsmouth

Appendix Five: Phase Two Interviews Information Sheet

Participant Information Sheet

Study Title: Information and Intelligence Sharing in the Fight Against Fraud

I would like to invite you to take part in my research study. Before you decide I would like you to understand why the research is being done and what it would involve for you. Talk to others about the study if you wish. Ask me if there is anything that is not clear.

This research is being conducted using the methods of qualitative research interviews and case study research. You are being invited to take part in a qualitative interview.

What is the purpose of the study?
This study is being conducted to research the issue of inter-organisational information and intelligence sharing in the prevention, detection and investigation of fraud. Information and intelligence sharing is a key strategy in combating fraud, and yet there are many challenges and obstacles that impede effective sharing between organisations in many sectors. This research seeks to examine how some of these challenges may be overcome. Furthermore, this research is being conducted as part of a doctoral degree programme at the University of Portsmouth, and the data collected will be presented in a thesis to be submitted by me in pursuance of a Professional Doctorate in Criminal Justice.

Why have I been invited?
You have been invited to take part in a qualitative research interview given your position in an organisation which is involved with issues relevant to information and intelligence sharing. As such, you are likely to have informed knowledge and views on this subject that would be helpful to the research.

If you agree to take part, you will be one of approximately twenty research interview participants within the study, who will be selected from different organisations.

Do I have to take part?
Participation in a research interview is entirely voluntary, and it is up to you to decide whether or not you wish to join the study. I will describe the study and go through this information sheet. If you do agree to participate, I will ask you to sign a consent form.

What will happen to me if I take part?
If you agree to join the study, you will take part in a qualitative research interview. This will be a one-off interview, which I anticipate should last approximately one hour. The interview will focus on issues of information and intelligence sharing for anti-fraud purposes. The information that you provide during the interview will be used solely for the stated research purpose outlined above. Neither your identity, nor that of your organisation, will be revealed

in any output from the research, unless you specifically request or consent for it to be revealed. Any information that you provide will not be presented in a way that will allow your responses to be linked with you individually.

If you agree to it, the interview will be recorded on a digital audio recording device in order to assist me in accurate collection and recall of the interview data.

Expenses and payments
In order to reduce any inconvenience to you in taking part in the research, I will travel to a location where it would be most convenient for you for the interview to be conducted (this may be your office or another location of your choice, although should be one that is relatively free from background noise).

I will reimburse any reasonable expenses that are incurred by you (e.g. for travel or refreshments) in taking part in the research.

What will I have to do?
As a research interview participant, the only requirement on your part would be to take part in the interview, and answer questions relevant to the research topic. There will be no ongoing requirement or commitment.

What are the possible disadvantages and risks of taking part?
The primary anticipated disadvantage of taking part in the research interview is the inconvenience to you in giving up your time to take part. Although I will take care to ensure that you cannot be identified in any output from the research, there remains an underlying risk that you might potentially be identifiable from any direct quotations used. This risk will be minimised as far as possible.

What are the possible benefits of taking part?
The primary anticipated benefit of your taking part is that you would be assisting in the conduct of the research, and will contribute to a greater understanding of the subject of the research.

Will my taking part in the study be kept confidential?
Although the subject matter of the research is not considered to be particularly sensitive in nature, the interviews will be conducted with a view to keeping the identities of participants, and the organisations for which they work, undisclosed (unless you or your organisation specifically choose and give express consent to be identified in output from the research).

If you join the study, it is possible that some of the data collected will be looked at by authorised persons from the University of Portsmouth, or external examiners in respect of the doctoral course. Data may also be looked at by authorised people to check that the study is being carried out correctly. All will have a duty of confidentiality to you as a research participant and will do their best to meet this duty.

The research data collected during the research interviews will be treated confidentially during the collection, analysis and examination process as identified below.

The research interviews will be digitally recorded if you consent to such recording. Recordings of interviews will be transcribed for subsequent analysis. Neither digital recordings, nor transcriptions, will contain details of your identity, other than in circumstances beyond my control (e.g. if you refer to your identity during a recorded interview).

Electronic data will be stored on a password protected computer to which I will have sole access, with a backup copy of data stored on a secure and protected external hard drive, again to which only I will have access. Written notes will be stored securely at my home address.

Data collected will be used only for the purposes of this research study and will not be retained or re-analysed for future research studies.

During the period of the doctoral programme for which this research is being conducted, access to the research data will normally be restricted to me. However, as the research is being conducted as part of an assessed educational programme, authorised persons such as my research supervisor, examiners and R&D auditors monitoring the quality of research, may require access to the data. Access will be restricted to those with a legitimate purpose relevant to the course of study and the examination process.

Data collected during the study, and any information that may identify the individual participants in the research, will be destroyed within thirty-one days after the course of study has ended. By this time, all electronic records of the research data collected during the case study (including interview recordings and transcripts) will be erased, as will the backup of the data. Paper-based records and notes will be shredded using a cross-cut shredder.

Until the data is destroyed, individual participants will have the right to access any data held about them to check it for accuracy if they wish to do so, and will be able to correct any mistakes. All data collected will be stored in accordance with the provisions of the Data Protection Act 1998.

Any reference to individual's responses, or direct quotations, used in output of the research (e.g. the doctoral thesis and any subsequently published materials), will not name the participant.

What will happen if I don't want to carry on with the study?

If you wish to withdraw from the study after indicating your willingness to take part, you may do so before or during the research interview, or immediately afterwards. However, once the interview data has been analysed and integrated with findings from other aspects of the research data gathering, it may not be possible to do so, so you should consider this when deciding whether or not you wish to take part.

If you do decide to withdraw, subject to the provisions above, any identifying information about you, and data that has already collected but not integrated into the study, will be destroyed within 31 days of your notifying me of your wish to withdraw. Any data already

collected and analysed as part of the wider study may be retained and used within the study, but will be destroyed within 31 days of the end of the course of study as outlined above.

What if there is a problem?
If you have a concern or complaint about any aspect of the research, or how it has been conducted by me, please ask me or my supervisor and we will do our best to answer your questions. The relevant contact details in these instances are:

Researcher: Carl Watson. Mobile: [redacted]. Email: carl.watson@myport.ac.uk

Supervisor: Professor Mark Button. Telephone: 02392 843923. Email: mark.button@port.ac.uk

If you remain unhappy and wish to complain formally, you can do this to the Head of the Institute of Criminal Justice Studies at the University of Portsmouth:

Head of ICJS: Dr Phil Clements. Telephone: 02392 845069. Email: phil.clements@port.ac.uk

What will happen to the results of the research study?
The results of the research will be analysed and incorporated into a thesis to be submitted to the University of Portsmouth for examination towards a doctoral degree award. If successful, the results may also be used in subsequent output for possible publication, such as in academic articles or a monograph. I will be willing to make available to you, as a participant, a digital copy of the thesis upon request. I would also be willing to provide you with, upon request, a summary of the findings of the research. You will not be identified in any such output.

Who is organising and funding the research?
The research is being conducted as part of a doctoral degree programme, and is being sponsored by the University of Portsmouth. The research is not being externally funded by way of any research grant.

Who has reviewed the study?
Research in the University of Portsmouth is looked at by independent group of people, called an Ethics Committee, to protect your interests. This study has been reviewed and given a favourable opinion by the Faculty Ethics Committee of the Humanities and Social Sciences faculty at the University of Portsmouth.

Further information and contact details
If you wish to obtain further information about this research, please contact me or my research supervisor in the first instance. Our contact details are as follows:

Researcher: Carl Watson. Mobile: [redacted]. Email: carl.watson@myport.ac.uk

Supervisor: Professor Mark Button. Telephone: 02392 843923. Email: mark.button@port.ac.uk

Concluding statement

Thank you for reading this information sheet, and for considering whether or not you wish to take part in this research study. If you decide to participate in the study, you will be given a copy of this information sheet to retain, and you will be asked for your formal consent to take part.

Appendix Six: Phase Two Interviews Consent Form

Consent Form

Study Title: ..Information and Intelligence Sharing in the Fight Against Fraud.....

FHSS REC Ref No: .....

Name of Researcher: .Carl Watson..... **Please initial box**

1.	I confirm that I have read and understand the information sheet dated.. ..... (version CW/RI/1) for the above study. I have had the opportunity to consider the information, ask questions and have had these answered satisfactorily.	☐
2.	I understand that my participation is voluntary and that I am free to withdraw at any time up to the point where the data are analysed without giving any reason.	☐
3.	I agree to my interview being audio recorded on a digital recording device.	☐
4.	I agree to being quoted verbatim, and have been informed that my identity will not be disclosed where I am quoted.	☐
6.	I agree to take part in the above study.	☐

Name of Participant: Date: Signature:

Name of Person taking consent : Date: Signature:

When completed: 1 for participant; 1 for researcher 's file.

Date: Version No. CW/RI/1

Appendix Seven: Phase One Case Study Invitation Letter

Study Title: Information and Intelligence Sharing in the Fight Against Fraud

FHSS REC Ref No: .....

Dear Potential Participant

I would like to invite [organisation name] to participate in a research case study into the subject of anti-fraud information and intelligence sharing. As an anti-fraud professional, I recognise [organisation name] as an organisation involved in information and intelligence sharing for anti-fraud purpose.

I am a postgraduate research student at the Institute of Criminal Justice Studies at the University of Portsmouth, taking a Professional Doctorate in Criminal Justice course. For this degree course, I am conducting research into anti-fraud information and intelligence sharing, with a view to increasing understanding of inter-organisational collaboration and how to overcome the challenges that impede it.

I believe that [organisation name] might be a suitable participant in my research as a case study. Further to the discussions that we have already had with respect to the nature of the case study, and what it would involve, I have enclosed with this letter a Participant Information Sheet containing further details of the research. If you wish to take part in the study, I would request that you confirm that you are willing to do so, and I have provided my contact details below. Prior to the commencement of the case study research, I will ask you to complete and sign a Consent Form, a copy of which is enclosed for your information. I will bring copies of this to be signed on the first day of the study.

My contact details are:

Carl Watson
[redacted]

Email: carl.watson@myport.ac.uk

Mobile: [redacted]

The participation in the case study research, by both [organisation name] and any officers and employees of the organisation, is entirely voluntary. Withdrawal from participation can readily be made prior to completion of the case study research, although may not be possible once the research has been completed and the data analysed. If you do wish to withdraw, please inform the researcher.

Date: Version No. CW/CS/1

Thank you for reading this letter, regardless of whether or not you choose to take part in the study.

Yours sincerely

Carl Watson
Postgraduate Research Student
University of Portsmouth

Date: Version No. CW/CS/1

Appendix Eight: Phase One Case Study Information Sheet

Participant Information Sheet

Study Title: Information and Intelligence Sharing in the Fight Against Fraud

I would like to invite your organisation to take part in my research study. Before you decide I would like you to understand why the research is being done and what it would involve for your organisation. Talk to others about the study if you wish. Ask me if there is anything that is not clear.

This research is being conducted using the methods of qualitative research interviews and case study research. [Organisation name] is being invited to take part as the subject of a case study.

What is the purpose of the study?
This study is being conducted to research the issue of inter-organisational information and intelligence sharing in the prevention, detection and investigation of fraud. Information and intelligence sharing is a key strategy in combating fraud, and yet there are many challenges and obstacles that impede effective sharing between organisations in many sectors. This research seeks to examine how some of these challenges may be overcome. Furthermore, this research is being conducted as part of a doctoral degree programme at the University of Portsmouth, and the data collected will be presented in a thesis to be submitted by me in pursuance of a Professional Doctorate in Criminal Justice.

Why have I been invited?
You have been invited to take part as I believe that [Organisation Name] will make an ideal case study of an organisation that currently utilises and shares information and intelligence with others to combat fraud. This view was reinforced following preliminary discussions with you about the research project. [Organisation Name] will be one of only one or two case studies conducted within this research, although additional interviews will be sought with other organisations in a different stage of the project. None of the information obtained from the case study research conducted with you will be discussed or disclosed to other participants in the project.

Do we have to take part?
Your participation in the research, should you wish to take part, is entirely voluntary, and there is no obligation upon you to take part. Furthermore, as the case study will involve our seeking information from employees within [Organisation Name], the involvement of any employees' in the research will also be entirely voluntary.
I will provide you with details and information about the study in order that you may make an informed choice about your involvement. If you do agree to participate, I will ask you to sign a consent form.

What will happen if we take part?
The case study will involve me conducting detailed research into the organisation as a relevant case of an organisation sharing information and intelligence for anti-fraud purposes. As such, this will entail me engaging in a variety of tasks methods to gather data, with the agreement of the organisation. Such methods will include examining documents, policies and protocols, conducting interviews with officers and staff members (subject to the informed consent of these individuals), and my spending an agreed period of time onsite at [organisation name]'s operational sites as an observer.

Information about the organisation, and its operating model in respect of information and intelligence usage and sharing, will necessarily be gathered during the research, although confidential identifying information relating to operational issues (for example, the subject of investigations or intelligence) will not be recorded or used. Furthermore, while as a case study it will be necessary to identify the organisation in the research and output from it, no personal information about employees will be retained or used in any output from the research. Interviews with officers and staff will, subject to each individual participant's consent, be digitally recorded in order to assist information capture and recall. The content of these will be treated confidentially and will not normally be shared with [organisation name] other than in any specific circumstances that limit the confidentiality, such as where information arises that threatens or harms the organisation. Any such circumstances and limitations will be agreed with [organisation name] by way of a protocol to be agreed before the interviews commence. I may also make, again subject to the agreement of [organisation name], intermittent audio 'logs' during the period of onsite observation during the research. No video recording or photography will be undertaken during any part of the case study research.

As the output of the case study research will identify the organisation, I will require the specific consent of an appropriately senior officer for this to be allowed.

What will we have to do?
As the participant in the case study, the cooperation of [organisation name] in facilitating my access to agreed documents, staff (with their permission) and access to the facility during the periods of onsite research as an observer will be necessary. Such access will be subject to agreement between [organisation name] and me as the researcher as to what will be reasonable, appropriate, relevant and acceptable levels of access to the organisation and its facilities and resources.

What are the possible disadvantages and risks of taking part?
As the participant in a case study, there are potential risks for the organisation of which it should be aware. Firstly, as mentioned above, the organisation will necessarily be identified as the subject of the case study in output from the research, which will be an academic thesis and, potentially, subsequent publications (such as articles or monographs) reporting on the research and its findings. There is, therefore, a potential for impact upon the organisation's reputation associated with this. While the organisation's identity will be disclosed in the thesis, and perhaps subsequent output, employees and officers identities will not be disclosed in any way.

Secondly, as a case study participant, there will be an impact upon the organisation in terms of its facilitation of the research through my spending time on site with officers and employees, although efforts will be taken to minimise any inconvenience caused.

Additionally, as the case study research will involve the me spending time onsite with officers and staff, there is a risk that I may be exposed to confidential or sensitive information about [organisation name]'s operations, including with regards to suspected criminals. I will not actively take notes that identify such sensitive information but, if such data is obtained during exposure to it, it will not be disclosed in any output from the research, as this will be concerned with the processes of information and intelligence sharing and handling. I will be willing to sign relevant confidentiality agreements that [organisation name] may wish to set up in respect of such risks.

What are the possible benefits of taking part?
The primary anticipated benefit of the organisation taking part is that it would be assisting in the conduct of the research, and will contribute to a greater understanding of the subject of the research. There could be additional potential benefits to the organisation in taking part in the case study research through insights arising from the research from the application of my research perspective of the organisation and its information and intelligence sharing model.

Will my taking part in the study be kept confidential?
As the subject of a case study, it will be necessary to disclose the name of the organisation within the output of the research.

The names of employees of the organisation will not be disclosed and will be treated with discretion within all output from the research. However, as the organisation will be identified, there may be a risk that the identity of some participants, especially where those staff members' association with the organisation is in the public domain, may be guessed or inferred by some who read the output of the research. This possibility will be minimised to the greatest possible extent.

If your organisation joins the study, it is possible that some of the data collected will be looked at by authorised persons from the University of Portsmouth, or external examiners in respect of the doctoral course. Data may also be looked at by authorised people to check that the study is being carried out correctly. All will have a duty of confidentiality to you as a research participant and will do their best to meet this duty.

The research data collected during the case study about [organisation name] and individual participants will be treated confidentially during the collection, analysis and examination process as identified below.

Data will be collected through means of document analysis, interview and researcher observation. I will take written, and possibly digitally recorded oral, notes, and interviews will be digitally recorded (with the interviewee's consent). Recordings of interviews will be transcribed for subsequent analysis. Neither digital recordings, nor transcriptions, will contain details of the interviewer's identity, other than in circumstances beyond my control (e.g. if the interviewee refers to their identity on a recorded interview).

Electronic data will be stored on a password protected computer to which only I have access, with a backup copy of data stored on a secure and protected external hard drive, again to which only I will have access. Written notes will be stored securely at my home address.

Data collected will be used only for the purposes of this research study and will not be retained or re-analysed for future research studies.

During the period of the doctoral programme for which this research is being conducted, access to the research data will normally be restricted to me. However, as the research is being conducted as part of an assessed educational programme, authorised persons such as my research supervisor, examiners and R&D auditors monitoring the quality of research, may require access to the data. Access will be restricted to those with a legitimate purpose relevant to the course of study and the examination process.

Data collected during the study, and any information that may identify the individual participants in the research, will be destroyed within thirty-one days after the course of study has ended. By this time, all electronic records of the research data collected during the case study (including interview recordings and transcripts) will be erased, as will the backup of the data. Paper-based records and notes will be shredded using a cross-cut shredder.

Until the data is destroyed, individual participants will have the right to access any data held about them to check it for accuracy if they wish to do so, and will be able to correct any mistakes. [Organisation name] will have the right to access the information held about it and to correct any mistakes, although for confidentiality reasons it will not have access to digital recordings, or transcripts, of interviews with individual participants. All data collected will be stored in accordance with the provisions of the Data Protection Act 1998.

What will happen if we don't want to carry on with the study?
[Organisation name] will have the right to withdraw from participation in the case study before data collection has commenced, and will be able to end participation before it has been completed. Likewise, employees who consent to being interviewed as part of the case study will also have the right to withdraw prior to, or during, the interview. In both cases, it may not be possible to withdraw after data has been collected and analysed.
Where such withdrawal is made, any data that has been collected that can be isolated from the wider research study and findings will be destroyed within 31 days of my being notified of the withdrawal. Any data already collected and analysed as part of the wider study may be retained and used within the study, but will be destroyed within 31 days of the end of the course of study as outlined above.

What if there is a problem?
If [organisation name] or any individual participants in the case study research have a concern or complaint about any aspect of the research, or how it has been conducted by me, please ask me or my supervisor and we will do our best to answer your questions. The relevant contact details in these instances are:

Researcher: Carl Watson. Mobile: [redacted]. Email: carl.watson@myport.ac.uk

Supervisor: Professor Mark Button. Telephone: 02392 843923. Email: mark.button@port.ac.uk

If you remain unhappy and wish to complain formally, you can do this to the Head of the Institute of Criminal Justice Studies at the University of Portsmouth:

Head of ICJS: Dr Phil Clements. Telephone: 02392 845069. Email: phil.clements@port.ac.uk

What will happen to the results of the research study?
The results of the case study research will be analysed and incorporated into a thesis to be submitted to the University of Portsmouth for examination towards a doctoral degree award. If successful, the results may also be used in subsequent output for possible publication, such as in academic articles or a monograph. I will be willing to make available upon request to [organisation name] a digital copy of the thesis and to notify it of any subsequent output that I publish arising directly from the research within a two year period of the completion of the thesis. (I may not necessarily hold the copyright to any subsequently published material, and therefore cannot commit to being able to distribute copies of these). I would also be willing to provide a summary of the findings of the case study, and/or the full research, to the organisation, or to employees who have assisted in the study, upon request. The organisation will necessarily be identified in such output, but no individuals will be identified unless they have given their consent.

Who is organising and funding the research?
The research is being conducted as part of a doctoral degree programme, and is being sponsored by the University of Portsmouth. The research is not being externally funded by way of any research grant, but is being personally funded.

Who has reviewed the study?
Research in the University of Portsmouth is looked at by independent group of people, called an Ethics Committee, to protect your interests. This study has been reviewed and given a favourable opinion by the Faculty Ethics Committee of the Humanities and Social Sciences faculty at the University of Portsmouth.

Further information and contact details
If you wish to obtain further information about this research, please contact me or my research supervisor in the first instance. Our contact details are as follows:

Researcher: Carl Watson. Mobile: [redacted]. Email: carl.watson@myport.ac.uk

Supervisor: Professor Mark Button. Telephone: 02392 843923. Email: mark.button@port.ac.uk

Concluding statement
Thank you for reading this information sheet, and for considering whether or not you wish to take part in this research study. If you decide to participate in the study, you will be given a copy of this information sheet to retain, and you will be asked for your formal consent to take part.

Appendix Nine: Preliminary Consent Letter (pre-Ethics Approval) – FACT

Federation Against Copyright Theft Ltd
Europa House • Church Street
Old Isleworth • Middlesex • TW7 6DA

t: +44 (0)20 8568 6646
f: +44 (0)20 8560 6364

w: www.fact-uk.org.uk
e: contact@fact-uk.org.uk

29 October 2013

Study Title: Information and Intelligence Sharing in the Fight Against Fraud

FHSS REC Ref No: [Ethical Approval Pending]

Name of Researcher: Carl Watson

Dear Sir or Madam

This letter confirms my willingness, in principle, for the Federation Against Copyright Theft (FACT) to be the subject of a research case study into anti-fraud information and intelligence sharing being conducted by Carl Watson for the purposes of his Professional Doctorate course at the University of Portsmouth.

During preliminary discussions, Carl and I have discussed some of the implications of our participation in the study, and the methods that will be used to conduct the research. These will include Carl conducting interviews with staff and officers (subject to their consent), examining our documents and processes relevant to the processing and exchange of information and intelligence, and his spending some time with the organisation as an observer.

It has been made clear that, as a research case study, FACT will be named in the output from the research.

This letter gives indicative consent on FACT's behalf to take part in the research, although I understand that at the time of this letter, the research is still awaiting Ethical Approval from the Faculty Ethics Committee. Once this approval has been obtained, I understand that I will be asked to provide formal consent on behalf of FACT. As such, there is no obligation arising from the agreement in principle given in this letter.

Yours sincerely

Kieron Sharp
Director General

FACT Working in partnership with the charity

CRIMESTOPPERS 0800 555 111

Crimestoppers is an independent charity

Registered in England No. 1672835
Registered Office as above

Appendix Ten: Phase One Case Study Consent Form

Consent Form

Study Title: ..Information and Intelligence Sharing in the Fight Against Fraud.....

FHSS REC Ref No: .....

Name of Researcher: .Carl Watson..... **Please initial box**

1. I confirm that I have read and understand the information sheet dated.. ..... (version CW/CS/1) for the above study. I have had the opportunity to consider the information, ask questions and have had these answered satisfactorily. ☐

2. I understand that my organisation's participation is voluntary and that it is free to withdraw at any time up to the point when the data are analysed without giving any reason. ☐

3. I agree to [organisation name] being the subject of a research case study, and it being a named participant and quoted by name. ☐

4. I agree to the researcher accessing and examining documents, systems, processes, protocols and other information relating to [organisation name] which are relevant to the subject of the study. ☐

5. I agree to the researcher interviewing, and conducting research with, officers and employees of [organisation name], subject to these persons giving their own consent to take part. By signing this consent form on behalf of [organisation name], no obligation is conferred upon officers or staff of the organisation to take part in the research. ☐

6. I agree to (organisation) taking part in the above study. ☐

Name of Participant: Date: Signature:

Position within [organisation name]:

Name of Person taking consent : Date: Signature:

When completed: 1 for participant; 1 for researcher 's file.

Date: Version No. CW/CS/1

Appendix Eleven: Phase One Interviews Invitation Letter

Study Title: ..Information and Intelligence Sharing in the Fight Against Fraud

FHSS REC Ref No: .....

Dear Potential Participant

I would like to invite you to participate in a research study into Information and Intelligence Sharing in the Fight Against Fraud.

I am a postgraduate research student at the Institute of Criminal Justice Studies at the University of Portsmouth, taking a Professional Doctorate in Criminal Justice course. For this degree course, I am conducting research into anti-fraud information and intelligence sharing, with a view to increasing understanding of inter-organisational collaboration and how to overcome the challenges that impede it.

I am inviting you to take part in a research interview as part of a wider case study being conducted into [organisation name] and its model and processes for sharing information and intelligence. As part of the case study, I am aiming to conduct interview research with employees of [organisation name] and think that you would be a suitable participant in this process. Whilst [organisation name] has agreed for me to conduct case study research into it, I wish to point out that this in no way places any obligation upon you to take part, and you can make the decision whether or not you wish to be involved in the study.

I have enclosed with this letter a Participant Information Sheet containing further details of the research. If you are willing to take part in the study, I would request that you confirm that you are willing to do so, and I have provided my contact details below. Prior to the commencement of the case study research, I will ask you to complete and sign a Consent Form, a copy of which is enclosed for your information. I will bring copies of this to be signed prior to the interview taking place..

My contact details are:

[redacted]

Email: carl.watson@myport.ac.uk

Mobile: [redacted]

Participation in the research is entirely voluntary. Withdrawal from participation can readily be made prior to completion of the case study research, although may not be possible once

Date: Version No. CW/CS/2

the research has been completed and the data analysed. If you do wish to withdraw, please inform the researcher using the contact details above.

Thank you for reading this letter, regardless of whether or not you choose to take part in the study.

Yours sincerely

Carl Watson
Postgraduate Research Student
University of Portsmouth

Date: Version No. CW/CS/2

Appendix Twelve: Phase One Interviews Information Sheet

Participant Information Sheet

Study Title: Information and Intelligence Sharing in the Fight Against Fraud

I would like to invite you to take part in my research study. Before you decide I would like you to understand why the research is being done and what it would involve for you. Talk to others about the study if you wish. Ask me if there is anything that is not clear.

This research is being conducted using the methods of qualitative research interviews and case study research. You are being invited to take part in a qualitative interview as part of the case study.

What is the purpose of the study?
This study is being conducted to research the issue of inter-organisational information and intelligence sharing in the prevention, detection and investigation of fraud. Information and intelligence sharing is a key strategy in combating fraud, and yet there are many challenges and obstacles that impede effective sharing between organisations in many sectors. This research seeks to examine how some of these challenges may be overcome. Furthermore, this research is being conducted as part of a doctoral degree programme at the University of Portsmouth, and the data collected will be presented in a thesis to be submitted by me in pursuance of a Professional Doctorate in Criminal Justice.

Why have I been invited?
You have been invited to take part in a qualitative research interview as part of a wider case study being conducted into anti-fraud information and intelligence sharing being conducted at, and with the consent of, [organisation name].

If you agree to take part, you will be one of several officers and employees of [organisation name] who will be interviewed as part of the case study research.

Do I have to take part?
Participation in a research interview is entirely voluntary, and it is up to you to decide whether or not you wish to join the study. I will describe the study and go through this information sheet. If you do agree to participate, I will ask you to sign a consent form.

While [organisation name] has agreed to take part in the research, I would like to point out that this in no way places any obligation upon you to take part, and it is up to you to decide whether or not you wish to participate as part of the case study.

What will happen to me if I take part?
If you agree to join the study, you will take part in a qualitative research interview. This will be a one-off interview, which I anticipate should take no more than one hour. The interview

will focus on issues of information and intelligence sharing for anti-fraud purposes, and how this is conducted within the context of [organisation name]. The information that you provide during the interview will be used solely for the stated research purpose outlined above. Your identity will not be revealed in any output from the research, unless you specifically request or consent for it to be revealed, although [organisation name] will be identified with the output of the research, and has agreed to be so named.

If you agree to it, the interview will be recorded on a digital audio recording device in order to assist me in accurate collection and recall of the interview data.

What will I have to do?
As a research interview participant, the only requirement on your part would be to take part in the interview, and answer questions relevant to the research topic. There will be no ongoing requirement or commitment.

What are the possible disadvantages and risks of taking part?
The primary anticipated disadvantage of taking part in the research interview is the inconvenience to you in giving up your time to take part. Subject to agreement with [organisation name], I would expect this to be in your normal working time, and I will clarify this prior to the interview taking place. Although I will take care to ensure that you cannot be identified in any output from the research, there remains an underlying risk that you might potentially be identifiable from any direct quotations used, especially if people know that you are employed at [organisation name]. This risk will be minimised as far as possible.

What are the possible benefits of taking part?
The primary anticipated benefit of your taking part is that you would be assisting in the conduct of the research, and will contribute to a greater understanding of the subject of the research.

Will my taking part in the study be kept confidential?
Although the subject matter of the research is not considered to be particularly sensitive in nature, the interviews will be conducted with a view to keeping the identities of interview participants undisclosed (unless you specifically choose and give express consent to be identified in output from the research).

The content of the research interviews will be treated as confidential, and under normal circumstances will not be disclosed or shared with [organisation name]. Any limits to this confidentiality, such as where information is disclosed during the research interview that may threaten or harm [organisation name] will be treated in accordance with a protocol to be agreed between me as the researcher and [organisation name], and you will be provided with a written summary of any such limitations prior to your taking part in an interview.

If you join the study, it is possible that some of the data collected will be looked at by authorised persons from the University of Portsmouth, or external examiners in respect of the doctoral course. Data may also be looked at by authorised people to check that the study is being carried out correctly. All will have a duty of confidentiality to you as a research participant and will do their best to meet this duty.

The research data collected during the research interviews will be treated confidentially during the collection, analysis and examination process as identified below.

The research interviews will be digitally recorded if you consent to such recording. Recordings of interviews will be transcribed for subsequent analysis. Neither digital recordings, nor transcriptions, will contain details of your identity, other than in circumstances beyond my control (e.g. if you refer to your identity during a recorded interview).

Electronic data will be stored on a password protected computer to which only I have access, with a backup copy of data stored on a secure and protected external hard drive, again to which only I will have access. Written notes will be stored securely at my home address.

Data collected will be used only for the purposes of this research study and will not be retained or re-analysed for future research studies.

During the period of the doctoral programme for which this research is being conducted, access to the research data will normally be restricted to me. However, as the research is being conducted as part of an assessed educational programme, authorised persons such as my research supervisor, examiners and R&D auditors monitoring the quality of research, may require access to the data. Access will be restricted to those with a legitimate purpose relevant to the course of study and the examination process.

Data collected during the study, and any information that may identify the individual participants in the research, will be destroyed within thirty-one days after the course of study has ended. By this time, all electronic records of the research data collected during the case study (including interview recordings and transcripts) will be erased, as will the backup of the data. Paper-based records and notes will be shredded using a cross-cut shredder.

Until the data is destroyed, individual participants will have the right to access any data held about them to check it for accuracy if they wish to do so, and will be able to correct any mistakes. All data collected will be stored in accordance with the provisions of the Data Protection Act 1998.

Any reference to individual's responses, or direct quotations, used in output of the research (e.g. the doctoral thesis and any subsequently published materials), will not name the participant.

What will happen if I don't want to carry on with the study?
If you wish to withdraw from the study after indicating your willingness to take part, you may do so before or during the research interview, or immediately afterwards. However, once the interview data has been analysed and integrated with findings from other aspects of the case study, it may not be possible to do so, so you should consider this when deciding whether or not you wish to take part.

If you do decide to withdraw, subject to the provisions above, any identifying information about you, and data that has already collected but not integrated into the study, will be

destroyed within 31 days of your notifying me of your wish to withdraw. Any data already collected and analysed as part of the wider study may be retained and used within the study, but will be destroyed within 31 days of the end of the course of study as outlined above.

What if there is a problem?
If you have a concern or complaint about any aspect of the research, or how it has been conducted by me, please ask me or my supervisor and we will do our best to answer your questions. The relevant contact details in these instances are:

Researcher: Carl Watson. Mobile: [redacted]. Email: carl.watson@myport.ac.uk

Supervisor: Professor Mark Button. Telephone: 02392 843923. Email: mark.button@port.ac.uk

If you remain unhappy and wish to complain formally, you can do this to the Head of the Institute of Criminal Justice Studies at the University of Portsmouth:

Head of ICJS: Dr Phil Clements. Telephone: 02392 845069. Email: phil.clements@port.ac.uk

What will happen to the results of the research study?
The results of the research will be analysed and incorporated into a thesis to be submitted to the University of Portsmouth for examination towards a doctoral degree award. If successful, the results may also be used in subsequent output for possible publication, such as in academic articles or a monograph. I will be willing to make available to you, as a participant, a digital copy of the thesis upon request. I would also be willing to provide you with, upon request, a summary of the findings of the research. You will not be identified in any such output.

Who is organising and funding the research?
The research is being conducted as part of a doctoral degree programme, and is being sponsored by the University of Portsmouth. The research is not being externally funded by way of any research grant, but is being personally funded.

Who has reviewed the study?
Research in the University of Portsmouth is looked at by independent group of people, called an Ethics Committee, to protect your interests. This study has been reviewed and given a favourable opinion by the Faculty Ethics Committee of the Humanities and Social Sciences faculty at the University of Portsmouth.

Further information and contact details
If you wish to obtain further information about this research, please contact me or my research supervisor in the first instance. Our contact details are as follows:

Researcher: Carl Watson. Mobile: [redacted]. Email: carl.watson@myport.ac.uk

Supervisor: Professor Mark Button. Telephone: 02392 843923. Email: mark.button@port.ac.uk

Concluding statement

Thank you for reading this information sheet, and for considering whether or not you wish to take part in this research study. If you decide to participate in the study, you will be given a copy of this information sheet to retain, and you will be asked for your formal consent to take part.

Appendix Thirteen: Phase One Interviews Consent Form

Consent Form

Study Title: ..Information and Intelligence Sharing in the Fight Against Fraud.....

FHSS REC Ref No: .....

Name of Researcher: .Carl Watson..... **Please initial box**

1.	I confirm that I have read and understand the information sheet dated.. ..... (version CW/CS/2) for the above study. I have had the opportunity to consider the information, ask questions and have had these answered satisfactorily.	☐
2.	I understand that my participation is voluntary and that I am free to withdraw at any time up to the point where the data are analysed without giving any reason.	☐
3.	I have been informed and understand that, although my participation has been sought as part of a case study to which [organisation name] has agreed to take part in, there is no obligation upon me to take part in the study.	☐
4.	I agree to my interview being audio recorded on a digital recording device.	☐
5.	I agree to being quoted verbatim, and have been informed that my identity will not be disclosed where I am quoted.	☐
6.	I agree to take part in the above study.	☐

Name of Participant: Date: Signature:

Name of Person taking consent : Date: Signature:

When completed: 1 for participant; 1 for researcher 's file.

Date: Version No. CW/CS/2

Appendix Fourteen: Phase One Observation Sessions Invitation Letter

Study Title: ..Information and Intelligence Sharing in the Fight Against Fraud

FHSS REC Ref No: .....

Dear Potential Participant

I would like to invite you to participate in a research study into Information and Intelligence Sharing in the Fight Against Fraud.

I am a postgraduate research student at the Institute of Criminal Justice Studies at the University of Portsmouth, taking a Professional Doctorate in Criminal Justice course. For this degree course, I am conducting research into anti-fraud information and intelligence sharing, with a view to increasing understanding of inter-organisational collaboration and how to overcome the challenges that impede it.

I am inviting you to take part in my research as part of a wider case study being conducted into [organisation name] and its model and processes for sharing information and intelligence. As part of the case study, I am aiming to conduct observation (job shadowing) sessions with employees of [organisation name] and think that you would be a suitable participant in this process. Whilst [organisation name] has agreed for me to conduct case study research into it, I wish to point out that this in no way places any obligation upon you to take part, and you can make the decision whether or not you wish to be involved in the study.

I have enclosed with this letter a Participant Information Sheet containing further details of the research. If you are willing to take part in the study, I would request that you confirm that you are willing to do so, and I have provided my contact details below. Prior to the commencement of the case study research, I will ask you to complete and sign a Consent Form, a copy of which is enclosed for your information. I will bring copies of this to be signed prior to the observation session taking place..

My contact details are:

Carl Watson
[redacted]

Email: carl.watson@myport.ac.uk

Mobile: [redacted]

Participation in the research is entirely voluntary. Withdrawal from participation can readily be made prior to completion of the case study research, although may not be possible once

Date: Version No. CW/CS/3

the research has been completed and the data analysed. If you do wish to withdraw, please inform the researcher using the contact details above.

Thank you for reading this letter, regardless of whether or not you choose to take part in the study.

Yours sincerely

Carl Watson
Postgraduate Research Student
University of Portsmouth

Date: Version No. CW/CS/3

Appendix Fifteen: Phase One Observation Sessions Information Sheet

Participant Information Sheet

Study Title: Information and Intelligence Sharing in the Fight Against Fraud

I would like to invite you to take part in my research study. Before you decide I would like you to understand why the research is being done and what it would involve for you. Talk to others about the study if you wish. Ask me if there is anything that is not clear.

This research is being conducted using the methods of qualitative research interviews and case study research. You are being invited to take part in observational research as part of the case study.

What is the purpose of the study?
This study is being conducted to research the issue of inter-organisational information and intelligence sharing in the prevention, detection and investigation of fraud. Information and intelligence sharing is a key strategy in combating fraud, and yet there are many challenges and obstacles that impede effective sharing between organisations in many sectors. This research seeks to examine how some of these challenges may be overcome. Furthermore, this research is being conducted as part of a doctoral degree programme at the University of Portsmouth, and the data collected will be presented in a thesis to be submitted by me in pursuance of a Professional Doctorate in Criminal Justice.

Why have I been invited?
You have been invited to take part in the case study research being conducted into anti-fraud information and intelligence sharing being conducted at, and with the consent of, [organisation name]. Your position within the organisation would make you a suitable candidate to take part in the research.

Do I have to take part?
Participation in the research is entirely voluntary, and it is up to you to decide whether or not you wish to join the study. I will describe the study and go through this information sheet. If you do agree to participate, I will ask you to sign a consent form.

While [organisation name] has agreed to take part in the research, I would like to point out that this in no way places any obligation upon you to take part, and it is up to you to decide whether or not you wish to participate as part of the case study.

What will happen to me if I take part?
If you agree to join the study, I would seek to observe the work that you undertake in the course of your routine duties in order to build an understanding of how the organisation operates within the context of the use and exchange of information and intelligence. This would involve my accompanying you in the workplace for several hours over one or two sessions, observing the work that you undertake, and asking relevant questions about the role, systems and processes. The information that you provide during the period of

observation will be used solely for the stated research purpose outlined above. Your identity will not be revealed in any output from the research, unless you specifically request or consent for it to be revealed, although [organisation name] will be identified with the output of the research, and has agreed to be so named.

What will I have to do?
As a research participant, the your participation would entail your allowing me to observe you for a few hours while you work, and to help me to understand the processes that you follow within the context of the organisation's work and the theme of the use and sharing of information and intelligence. There will be no ongoing requirement or commitment other than the session, or sessions, in which I shadow your work.

What are the possible disadvantages and risks of taking part?
The primary anticipated disadvantage of taking part in the observational research is the inconvenience to you in allowing me to observe your work and ask questions during this time. Although I will take care to ensure that you cannot be identified in any output from the research, there remains an underlying risk that you might potentially be identifiable from any account of the work that is observed, especially if people know that you are employed at [organisation name] and the function that you perform there. This risk will be minimised as far as possible.

What are the possible benefits of taking part?
The primary anticipated benefit of your taking part is that you would be assisting in the conduct of the research, and will contribute to a greater understanding of the subject of the research.

Will my taking part in the study be kept confidential?
Although the subject matter of the research is not considered to be particularly sensitive in nature, the observations will be conducted with a view to keeping the identities of participants undisclosed (unless you specifically choose and give express consent to be identified in output from the research).

The data collected during the research observation sessions will be treated as confidential, and under normal circumstances will not be disclosed or shared with [organisation name]. Any limits to this confidentiality, such as where information is disclosed during the research observation session that may threaten or harm [organisation name] will be treated in accordance with a protocol to be agreed between me as the researcher and [organisation name], and you will be provided with a written summary of any such limitations prior to your taking part in the session.

If you join the study, it is possible that some of the data collected will be looked at by authorised persons from the University of Portsmouth, or external examiners in respect of the doctoral course. Data may also be looked at by authorised people to check that the study is being carried out correctly. All will have a duty of confidentiality to you as a research participant and will do their best to meet this duty.

The research data collected during the observation sessions will be treated confidentially during the collection, analysis and examination process as identified below.

Electronic data will be stored on a password protected computer to which I have sole access, with a backup copy of data stored on a secure and protected external hard drive, again to which only I will have access. Written notes will be stored securely at my home address.

Data collected will be used only for the purposes of this research study and will not be retained or re-analysed for future research studies.

During the period of the doctoral programme for which this research is being conducted, access to the research data will normally be restricted to me. However, as the research is being conducted as part of an assessed educational programme, authorised persons such as my research supervisor, examiners and R&D auditors monitoring the quality of research, may require access to the data. Access will be restricted to those with a legitimate purpose relevant to the course of study and the examination process.

Data collected during the study, and any information that may identify the individual participants in the research, will be destroyed within thirty-one days after the course of study has ended. By this time, all electronic records of the research data collected during the case study will be erased, as will the backup of the data. Paper-based records and notes will be shredded using a cross-cut shredder.

Until the data is destroyed, individual participants will have the right to access any data held about them to check it for accuracy if they wish to do so, and will be able to correct any mistakes. All data collected will be stored in accordance with the provisions of the Data Protection Act 1998.

Any reference to the observational data used in any output of the research (e.g. the doctoral thesis and any subsequently published materials), will not name the participant.

What will happen if I don't want to carry on with the study?
If you wish to withdraw from the study after indicating your willingness to take part, you may do so before or during the observation session(s), or immediately afterwards. However, once the research data has been analysed and integrated with findings from other aspects of the case study, it may not be possible to do so, so you should consider this when deciding whether or not you wish to take part.

If you do decide to withdraw, subject to the provisions above, any identifying information about you, and data that has already collected but not integrated into the study, will be destroyed within 31 days of your notifying me of your wish to withdraw. Any data already collected and analysed as part of the wider study may be retained and used within the study, but will be destroyed within 31 days of the end of the course of study as outlined above.

What if there is a problem?
If you have a concern or complaint about any aspect of the research, or how it has been conducted by me, please ask me or my supervisor who will do our best to answer your questions. The relevant contact details in these instances are:

Researcher: Carl Watson. Mobile: [redacted]. Email: carl.watson@myport.ac.uk

Supervisor: Professor Mark Button. Telephone: 02392 843923. Email: mark.button@port.ac.uk

If you remain unhappy and wish to complain formally, you can do this to the Head of the Institute of Criminal Justice Studies at the University of Portsmouth:

Head of ICJS: Dr Phil Clements. Telephone: 02392 845069. Email: phil.clements@port.ac.uk

What will happen to the results of the research study?
The results of the research will be analysed and incorporated into a thesis to be submitted to the University of Portsmouth for examination towards a doctoral degree award. If successful, the results may also be used in subsequent output for possible publication, such as in academic articles or a monograph. I will be willing to make available to you, as a participant, a digital copy of the thesis upon request. I would also be willing to provide you with, upon request, a summary of the findings of the research. You will not be identified in any such output.

Who is organising and funding the research?
The research is being conducted as part of a doctoral degree programme, and is being sponsored by the University of Portsmouth. The research is not being externally funded by way of any research grant, but is being funded personally.

Who has reviewed the study?
Research in the University of Portsmouth is looked at by independent group of people, called an Ethics Committee, to protect your interests. This study has been reviewed and given a favourable opinion by the Faculty Ethics Committee of the Humanities and Social Sciences faculty at the University of Portsmouth.

Further information and contact details
If you wish to obtain further information about this research, please contact me or my research supervisor in the first instance. Our contact details are as follows:

Researcher: Carl Watson. Mobile: [redacted]. Email: carl.watson@myport.ac.uk

Supervisor: Professor Mark Button. Telephone: 02392 843923. Email: mark.button@port.ac.uk

Concluding statement
Thank you for reading this information sheet, and for considering whether or not you wish to take part in this research study. If you decide to participate in the study, you will be given a copy of this information sheet to retain, and you will be asked for your formal consent to take part.

Appendix Sixteen: Phase One Observation Sessions Consent Form

Study Title: ..Information and Intelligence Sharing in the Fight Against Fraud.....

FHSS REC Ref No: .....

Name of Researcher: .Carl Watson..... **Please initial box**

1.	I confirm that I have read and understand the information sheet dated.. ..... (version CW/CS/3) for the above study. I have had the opportunity to consider the information, ask questions and have had these answered satisfactorily.	☐
2.	I understand that my participation is voluntary and that I am free to withdraw at any time up to the point where the data are analysed without giving any reason.	☐
3.	I have been informed and understand that, although my participation has been sought as part of a case study to which [organisation name] has agreed to take part in, there is no obligation upon me to take part in the study.	☐
4.	I agree to the researcher observing/shadowing my work within [organisation name] as part of the research case study.	☐
5.	I agree to take part in the above study.	☐

Name of Participant: Date: Signature:

Name of Person taking consent : Date: Signature:

When completed: 1 for participant; 1 for researcher 's file.

Date: Version No. CW/CS/3

Appendix Seventeen: Phase One Interview Schedules

Various version of the semi-structured interview schedule were produced for the following job roles within FACT (listed in the order reproduced in this appendix):

- Criminal Justice Officer
- Director General
- Director of Investigations and Intelligence
- Field Investigator
- Forensic Examiner
- Human Resources
- Intelligence Analyst
- Intelligence Manager
- Intelligence Researcher
- Internet Investigator
- Internet Researcher
- Internet Supervisor
- Investigations Manager
- ISP Liaison Officer
- IT Support
- Legal Counsel
- Market Strategist

Interview Schedule: Criminal Justice Officer

PREAMBLE: This interview is being conducted as part of case study research into information and intelligence sharing at the Federation Against Copyright Theft. The case study itself is part of a wider piece of doctoral research into anti-fraud information and intelligence sharing.

The interview is entirely voluntary, and your identity as a participant will not be disclosed in any output detailing the findings of the research. This interview is being recorded – please could you confirm that you consent to its being recorded? Thank you.

ABOUT YOUR ROLE

1. What is your job title?

2. Please could you give me an overview of your role within FACT?
   What do you do?
   How do you go about it?
   Typical day / Regular tasks
   Systems & Processes Used
   Output and production

ABOUT YOUR TEAM

3. How does your role fit in with the rest of your team?
   Working with others (vertically / horizontally)
   Interaction / Communication
   How is team organised?

4. How are your working goals and objectives set?
   How set, and who by?
   How are they measured?

5. How does the work that your team does fit in with the overall work of FACT?
   Goals
   Case work
   Interaction (working together)
   Formal / informal channels or processes for working with other teams?

6. How would you assess the role that intelligence and information plays within the way that FACT operates?
   Importance

CASE MANAGEMENT SYSTEM

7. Please could you give me an overview of the case management system, which I understand you h*ave responsibility for?*
   What system is it?
   How is it used?
   Who has access?
   Input procedures
   Outputs

INTELLIGENCE AND INFORMATION ANALYSIS AND USE

8. How do you use information and intelligence within your work?
   Daily basis
   Investigations / case work
   Other uses

9. How does intelligence and information that you use in your work reach you?
   Where from (internally / externally)?
   In what forms does it reach you (formal reports / briefings / email / phone / meetings etc)
   Is it pre-assessed by others first?

10. Do you, or the organisation, use any criteria or system to evaluate or grade the quality of information and intelligence gathered, shared or received?
    You
    FACT
    Internally sourced / developed intelligence
    Externally sourced / developed intelligence
    Can it be relied upon?

INTELLIGENCE SHARING

11. Do you deal with other organisations in the operational work that you do – those with which FACT shares information or intelligence?
    To what extent?
    What is your involvement?
    How do you manage these relationships?
    Incoming intelligence - processes
    Outgoing intelligence - processes

12. From your experience, how well does intelligence sharing work at FACT?
    Why?

13. Are there any problems that you experience in intelligence sharing with other organisations?
    What are these?
    Any particularly good or bad organisations?
    Is there enough sharing?
    Technical issues

Cultural Issues
Political Issues

14. How would you rate the culture within FACT with respect to intelligence handling and sharing?
    Why?
    Any way it could be improved?

Restrictions

15. Do you or your place any restrictions or conditions upon the information and intelligence shared with partners, and are you able to outline these?
    Onward sharing of information and intelligence (within or outside of network)

16. Are there any circumstances in which you or the organisation would be unwilling to share information / intelligence with other parties?
    What are these?
    What would need to change in order to allow or enable sharing?

17. Are there any circumstances in which your team would be unwilling to receive or process information / intelligence from other parties?
    What are these?
    What would need to change in order to allow or enable sharing?

CASES

18. Would you be able to talk me through an example of a case, or cases, that you have worked on where intelligence or information sourced from partner organisations has played a role?
    Overview of the case and situation?
    How did it come to light?
    What was your role?
    How did information or intelligence play a part in the case?
    Where did the information or intelligence come from?
    How was it identified – (e.g. volunteered by partner or requested by FACT?)
    How was it used?
    Outcome of case?
    Feedback to partner organisation?

FINAL

19. Is there anything that you would like to see done to better facilitate effective information and intelligence sharing in future (with respect to FACT, or the UK in general)?
    Changes to legislation
    System of licensing for those who hold and share data
    Training/accreditation
    Other

20. Are you aware of any good practice or innovation in this area, in the UK or overseas, that could be utilised more widely in the UK?

21. Is there anything more that you would like to add that we have not addressed?

[Closure – thank you for your time and participation]

Interview Schedule: Director General

PREAMBLE: This interview is being conducted as part of case study research into information and intelligence sharing at the Federation Against Copyright Theft. The case study itself is part of a wider piece of doctoral research into anti-fraud information and intelligence sharing.

The interview is entirely voluntary, and your identity as a participant will not be disclosed in any output detailing the findings of the research. This interview is being recorded – please could you confirm that you consent to its being recorded? Thank you.

ABOUT THE ORGANISATION

1. Please could you give me a broad overview of FACT, in terms of what it does and what it aims to achieve?
   Mission
   Aims
   Geographical focus/scope
   Main activities
   How successful is it in achieving goals?
   How do you measure success?

2. When was FACT established?

3. What type of organisation is it (e.g. private limited company)?
   Who owns/has an interest in it?
   Members

4. How is it funded?
   Income sources
   Profit seeking
   Level of funding/turnover

5. How many members of staff does it normally have?
   Other staff attached to organisation
   Outsourced functions and services

6. Please could you describe how the organisation is organised and run?
   General structure
   Leadership structure (e.g. board composition)
   Teams and functions
   Support functions

FACT'S WORK AND PRIMARY FUNCTIONS

7. Please could you outline the nature and scale of the threat(s) that the organisation tackles?
   Types of threat
   Types of perpetrator (criminals, citizens, location)
   Cost / impact in UK and globally
   Criminal / Civil
   What are the most significant threats, and why?

8. Very broadly speaking, how does it set out to achieve its mission?
   How does it approach the threats?
   What are the priorities for FACT to tackle?
   How are these priorities set?
   How does FACT adapt to changes in criminal tactics and methods?

9. From the organisational chart that you supplied, it appears to me that there are three main operational teams, these being an Intelligence Team under the Intelligence Manager, a Field Investigations team, under the Investigations Manager, and an Internet Investigations team, also under the Investigations Manager. Is this an accurate interpretation?

10. What is the function of the Intelligence Team?
    Structure
    Purpose
    How does it go about its work?
    How does this contribute to the organisation's work?
    How does the team work with other aspects of the organisation?

11. What is the function of the Field Investigations Team?
    Structure
    Purpose
    How does it go about its work?
    How does this contribute to the organisation's work?
    How does the team work with other aspects of the organisation?

12. What is the function of the Internet Investigations Team?
    Structure
    Purpose
    How does it go about its work?
    How does this contribute to the organisation's work?
    How does the team work with other aspects of the organisation?

13. Please could you provide me with a general overview of the additional and support functions that exist within FACT?
    ISP Liaison
    Legal Counsel

Financial Investigator
Admin
HR
Finance
IT
Any others

ABOUT YOUR ROLE

14. Please could you give me an overview of your own role within the organisation?
    What do you do?
    How do you go about it?
    How do you set strategy and objectives for the organisation?
    Involvement in individual cases
    Involvement in establishing and maintaining relationships with partner organisations

INTELLIGENCE AND INFORMATION ANALYSIS AND USE

15. Does FACT have or use a formal definition for data, information or intelligence, or use any other distinction between them?
    What are these?

16. How does FACT seek to use information and intelligence within its work?
    Daily basis
    Investigations / case work
    Other uses
    Who does this?
    Intelligence outputs / products
    Are there different processes or standards for use of data, information or intelligence?

17. Does FACT have a formal approach or process to how it uses information or intelligence (e.g. NIM)?
    How is this translated into use?
    How does this serve the organisation?
    Benefits
    Drawbacks / problems

18. How does FACT gather and develop information and intelligence?
    What for?
    Who does this?
    How do they do it?

19. Does FACT use any criteria or system to evaluate or grade the quality of information and intelligence gathered, shared or received?
    Internally developed
    Shared – incoming
    Shared - outgoing
    How does this process work?
    Who performs this?

20. What systems (hardware/software) do you use to manage, process and use information and intelligence?

21. How do you evaluate how effectively FACT gathers and utilises information and intelligence?
    Formal process
    How
    Who
    How often
    How do you rate it at the moment?

RELATIONSHIPS WITH OTHER ORGANISATIONS

22. Would you be able to provide me with an overview of how your organisation shares information and/or intelligence with others for the prevention or investigation of IP theft or fraud?
    With whom does it share?
    How does it share?
    What does it share (e.g. raw data / information / intelligence / intelligence products)
    Does it work effectively?

23. How do you identify with whom FACT wishes to work?

24. How do you negotiate, establish and develop an information and intelligence sharing relationship with another organisation?
    Process
    Who is involved?
    Key steps
    Agreeing scope
    Any formal agreements?
    Any relationship managers / key points of contact etc?
    Length of process

25. How does FACT manage and maintain its relationships with its information sharing partners?
    Meetings
    Dedicated staff / points of contact
    Senior level relationships
    Process (formal or informal) to evaluate these relationships to ensure they're working

26. On a general basis, how effective do you find your information and intelligence sharing partnerships to be – do they work effectively?
    Does FACT have the right partners?
    Do they provide what FACT needs?
    Does FACT provide what they need?
    Are some partnerships better than others? Why?

Are there any characteristics of partnership organisations that are better or worse than others (e.g. by sector, industry etc)
Can you think of how these relationships can be improved further?
Any that are particularly effective?
Any that are particularly ineffective?
Are there any notable factors that you have seen that may affect how effective a relationship may be (e.g. sector, type of organisation, other factors)?

BARRIERS AND PROBLEMS TO INFORMATION SHARING

Technical

27. From FACT's experience, what have been the most significant technical challenges that have impeded, or that have had to be tackled in respect of, sharing information or intelligence with other organisations?
    Data formats
    Data quality
    Data volume
    Other technical issues

28. How has FACT overcome these challenges?

29. Do any technical barriers still exist that impede, or sometimes prevent, effective information or intelligence sharing with other organisations?

Political / Legal

30. What have been the most significant political or legal challenges that have impeded, or that have had to be tackled in respect of, sharing information or intelligence with other organisations?
    Financial
    Political
    Bureaucratic
    Standards
    Legislative
    Cross-jurisdictional

31. How has FACT overcome these challenges?

32. Do any political or legal barriers still exist that impede, or sometimes prevent, effective information or intelligence sharing with other organisations?

Organisational / Cultural

33. What have been the most significant organisational or cultural challenges that have impeded, or that have had to be tackled in respect of, sharing information or intelligence with other organisations?
    Unwillingness to share
    Lack of trust
    Lack of feedback
    Ownership of information / intelligence
    Information asymmetry
    Non-reciprocal information flow
    Lack of understanding of partners' needs'

34. How has FACT overcome these challenges?

35. Do any organisational or cultural barriers still exist that impede, or sometimes prevent, effective information or intelligence sharing with other organisations?

Restrictions

36. Does your organisation place any restrictions or conditions upon the information and intelligence shared with partners, and are you able to outline these?
    Onward sharing of information and intelligence (within or outside of network)

37. Are there any circumstances in which FACT would be unwilling to share information / intelligence with other parties?
    What are these?
    What would need to change in order to allow or enable sharing?

FINAL

38. Is there anything that you would like to see done to better facilitate effective information and intelligence sharing in future in the UK?
    Changes to legislation
    System of licensing for those who hold and share data
    Training/accreditation

39. Are you aware of any good practice or innovation in this area, in the UK or overseas, that could be utilised more widely in the UK?

40. Is there anything more that you would like to add that we have not addressed?

[Closure – thank you for your time and participation]

Interview Schedule: Director of Investigations and Intelligence

PREAMBLE: This interview is being conducted as part of case study research into information and intelligence sharing at the Federation Against Copyright Theft. The case study itself is part of a wider piece of doctoral research into anti-fraud information and intelligence sharing.

The interview is entirely voluntary, and your identity as a participant will not be disclosed in any output detailing the findings of the research. This interview is being recorded – please could you confirm that you consent to its being recorded? Thank you.

ABOUT YOUR ROLE

1. Please could you give me an overview of your own role within the organisation?
   What do you do?
   How do you go about it?
   How do you set objectives and priorities for your teams?
   Involvement in individual cases
   Involvement in establishing and maintaining relationships with partner organisations

ABOUT THE INVESTIGATIONS AND INTELLIGENCE FUNCTIONS OF FACT

2. Please could you give me a broad overview of the investigations and intelligence functions within FACT, in terms of what they do and what they aim to achieve?
   Roles
   Aims
   Scope
   Main activities
   How successful are they in achieving goals?
   How do you measure success?

3. How many members of staff are there within the teams for which you have responsibility?
   Intelligence Team
   Investigations Team
   Internet Investigations Team
   Other

4. What is the function of the Intelligence Team?
   Structure
   Purpose
   How does it go about its work?
   How does this contribute to the organisation's work?
   How does the team work with other aspects of the organisation?

5. What is the function of the Field Investigations Team?
   Structure
   Purpose

How does it go about its work?
How does this contribute to the organisation's work?
How does the team work with other aspects of the organisation?

6. What is the function of the Internet Investigations Team?
   Structure
   Purpose
   How does it go about its work?
   How does this contribute to the organisation's work?
   How does the team work with other aspects of the organisation?

INTELLIGENCE AND INFORMATION ANALYSIS AND USE

7. Does FACT have or use a formal definition for data, information or intelligence, or use any other distinction between them?
   What are these?

8. How does FACT seek to use information and intelligence within its work?
   Daily basis
   Investigations / case work
   Other uses
   Who does this?
   Intelligence outputs / products
   Are there different processes or standards governing use of data, information or intelligence?

9. Does FACT have a formal approach or process to how it uses information or intelligence (e.g. NIM)?
   How is this translated into use?
   How does this serve the organisation?
   Benefits
   Drawbacks / problems

10. How does FACT gather and develop information and intelligence?
    What for?
    Who does this?
    How do they do it?

11. Does FACT use any criteria or system to evaluate or grade the quality of information and intelligence gathered, shared or received?
    Internally developed
    Shared – incoming
    Shared - outgoing
    How does this process work?
    Any corroboration processes used?

12. What systems (hardware/software) do you use to manage, process and use information and intelligence?

13. What systems and tools do you use to gather and develop information and intelligence?
    Online

Offline
Analysis
Production of intelligence products

14. How do you evaluate how effectively FACT gathers and utilises information and intelligence?
    Formal process
    How
    Who
    How often
    How do you rate it at the moment?

RELATIONSHIPS WITH OTHER ORGANISATIONS

15. Would you be able to provide me with an overview of how your organisation shares information and/or intelligence with others for the prevention or investigation of IP theft or fraud?
    With whom does it share?
    How does it share?
    What does it share (e.g. raw data / information / intelligence / intelligence products)
    Does it work effectively?

16. How do you identify with whom FACT wishes to work?

17. How do you negotiate, establish and develop an information and intelligence sharing relationship with another organisation?
    Process
    Who is involved?
    Key steps
    Agreeing scope
    Any formal agreements?
    Any relationship managers / key points of contact etc?
    Length of process

18. How does FACT manage and maintain its relationships with its information sharing partners?
    Meetings
    Dedicated staff / points of contact
    Senior level relationships
    Process (formal or informal) to evaluate these relationships to ensure they're working

19. On a general basis, how effective do you find your information and intelligence sharing partnerships to be – do they work effectively?
    Does FACT have the right partners?
    Do they provide what FACT needs?
    Does FACT provide what they need?
    Are some partnerships better than others? Why?
    Are there any characteristics of partnership organisations that are better or worse than others (e.g. by sector, industry etc)
    Can you think of how these relationships can be improved further?
    Any that are particularly effective?

Any that are particularly ineffective?
Are there any notable factors that you have seen that may affect how effective a relationship may be (e.g. sector, type of organisation, other factors)?

20. How do you tend to share data / information / intelligence with partner organisations (e.g. set reporting formats / verbal reports / data transfers / intelligence products, etc)?
    Information and intelligence sharing inwards with partners
    Information and intelligence shared by FACT with partners
    Set out in agreements?
    How are different types dealt with?
    Any technical or other challenges with each different type / format?
    How do you understand your partners' information or intelligence needs? (e.g. agreements, feedback processes)
    Who makes the decisions to share / is there an authorisation process?

BARRIERS AND PROBLEMS TO INFORMATION SHARING

Technical

21. From FACT's perspective, what have been the most significant technical challenges that have impeded, or that have had to be tackled in respect of, sharing information or intelligence with other organisations?
    Data formats
    Data quality
    Data volume
    Other technical issues

22. How has FACT overcome these challenges?

23. Do any technical barriers still exist that impede, or sometimes prevent, effective information or intelligence sharing with other organisations?

Political / Legal

24. What have been the most significant political or legal challenges that have impeded, or that have had to be tackled in respect of, sharing information or intelligence with other organisations?
    Financial
    Political
    Bureaucratic
    Standards
    Legislative
    Cross-jurisdictional

25. How has FACT overcome these challenges?

26. Do any political or legal barriers still exist that impede, or sometimes prevent, effective information or intelligence sharing with other organisations?

Organisational / Cultural

27. What have been the most significant organisational or cultural challenges that have impeded, or that have had to be tackled in respect of, sharing information or intelligence with other organisations?
    Unwillingness to share
    Lack of trust
    Lack of feedback
    Ownership of information / intelligence
    Information asymmetry
    Non-reciprocal information flow
    Lack of understanding of partners' needs'

28. How has FACT overcome these challenges?

29. Do any organisational or cultural barriers still exist that impede, or sometimes prevent, effective information or intelligence sharing with other organisations?

Restrictions

30. Does your organisation place any restrictions or conditions upon the information and intelligence shared with partners, and are you able to outline these?
    Onward sharing of information and intelligence (within or outside of network)

31. Are there any circumstances in which FACT would be unwilling to share information / intelligence with other parties?
    What are these?
    What would need to change in order to allow or enable sharing?

32. Have any of FACT's partner organisations reported or complained about problems or concerns in the relationship with FACT?
    [If yes] What were the circumstances?
    What happened?

FINAL

33. Is there anything that you would like to see done to better facilitate effective information and intelligence sharing in future in the UK?
    Changes to legislation
    System of licensing for those who hold and share data
    Training/accreditation

34. Are you aware of any good practice or innovation in this area, in the UK or overseas, that could be utilised more widely in the UK?

35. Is there anything more that you would like to add that we have not addressed?

[Closure – thank you for your time and participation]

Interview Schedule: Field Investigator

PREAMBLE: This interview is being conducted as part of case study research into information and intelligence sharing at the Federation Against Copyright Theft. The case study itself is part of a wider piece of doctoral research into anti-fraud information and intelligence sharing.

The interview is entirely voluntary, and your identity as a participant will not be disclosed in any output detailing the findings of the research. This interview is being recorded – please could you confirm that you consent to its being recorded? Thank you.

ABOUT YOUR ROLE

1. What is your job title?

2. Please could you give me an overview of your role within FACT?
   What do you do?
   How do you go about it?
   Typical day / Regular tasks
   Systems & Processes Used
   Output and production

ABOUT YOUR TEAM

3. How does your role fit in with the rest of your team?
   Working with others (vertically / horizontally)
   Interaction / Communication
   How is team organised?

4. How are your working goals and objectives set?
   How set, and who by?
   How are they measured?

5. How does the work that your team does fit in with the overall work of FACT?
   Goals
   Case work
   Interaction (working together)
   Formal / informal channels or processes for working with other teams?

6. How would you assess the role that intelligence and information plays within the way that FACT operates?
   Importance

INTELLIGENCE AND INFORMATION ANALYSIS AND USE

7. How do you use information and intelligence within your work?
   Daily basis
   Investigations / case work

Other uses

8. How does intelligence and information that you use in your work reach you?
   Where from (internally / externally)?
   In what forms does it reach you (formal reports / briefings / email / phone / meetings etc)
   Is it pre-assessed by others first?

9. Do you, or the organisation, use any criteria or system to evaluate or grade the quality of information and intelligence gathered, shared or received?
   You
   FACT
   Internally sourced / developed intelligence
   Externally sourced / developed intelligence
   Can it be relied upon?

INTELLIGENCE SHARING

10. Do you deal with other organisations in the operational work that you do – those with which FACT shares information or intelligence?
    To what extent?
    What is your involvement?
    How do you manage these relationships?
    Incoming intelligence - processes
    Outgoing intelligence - processes

11. From your experience, how well does intelligence sharing work at FACT?
    Why?

12. Are there any problems that you experience in intelligence sharing with other organisations?
    What are these?
    Any particularly good or bad organisations?
    Is there enough sharing?
    Technical issues
    Cultural Issues
    Political Issues

13. How would you rate the culture within FACT with respect to intelligence handling and sharing?
    Why?
    Any way it could be improved?

Restrictions

14. Do you or your place any restrictions or conditions upon the information and intelligence shared with partners, and are you able to outline these?
    Onward sharing of information and intelligence (within or outside of network)

15. Are there any circumstances in which you or the organisation would be unwilling to share information / intelligence with other parties?
    What are these?
    What would need to change in order to allow or enable sharing?

16. Are there any circumstances in which your team would be unwilling to receive or process information / intelligence from other parties?
    What are these?
    What would need to change in order to allow or enable sharing?

CASES

17. Would you be able to talk me through an example of a case, or cases, that you have worked on where intelligence or information sourced from partner organisations has played a role?
    Overview of the case and situation?
    How did it come to light?
    What was your role?
    How did information or intelligence play a part in the case?
    Where did the information or intelligence come from?
    How was it identified – (e.g. volunteered by partner or requested by FACT?)
    How was it used?
    Outcome of case?
    Feedback to partner organisation?

FINAL

18. Is there anything that you would like to see done to better facilitate effective information and intelligence sharing in future (with respect to FACT, or the UK in general)?
    Changes to legislation
    System of licensing for those who hold and share data
    Training/accreditation
    Other

19. Are you aware of any good practice or innovation in this area, in the UK or overseas, that could be utilised more widely in the UK?

20. Is there anything more that you would like to add that we have not addressed?

[Closure – thank you for your time and participation]

Interview Schedule: Forensic Examiner

PREAMBLE: This interview is being conducted as part of case study research into information and intelligence sharing at the Federation Against Copyright Theft. The case study itself is part of a wider piece of doctoral research into anti-fraud information and intelligence sharing.

The interview is entirely voluntary, and your identity as a participant will not be disclosed in any output detailing the findings of the research. This interview is being recorded – please could you confirm that you consent to its being recorded? Thank you.

ABOUT YOUR ROLE

1. What is your job title?

2. Please could you give me an overview of your role within FACT?
   What do you do?
   How do you go about it?
   Typical day / Regular tasks
   Systems & Processes Used
   Output and production

ABOUT YOUR TEAM

3. How does your role fit in with the rest of your team?
   Working with others (vertically / horizontally)
   Interaction / Communication
   How is team organised?

4. How are your working goals and objectives set?
   How set, and who by?
   How are they measured?

5. How does the work that your team does fit in with the overall work of FACT?
   Goals
   Case work
   Interaction (working together)
   Formal / informal channels or processes for working with other teams?

6. How would you assess the role that intelligence and information plays within the way that FACT operates?
   Importance

INTELLIGENCE AND INFORMATION ANALYSIS AND USE

7. How do you use information and intelligence within your work?
   Daily basis
   Investigations / case work
   Other uses

8. How does intelligence and information that you use in your work reach you?
   Where from (internally / externally)?
   In what forms does it reach you (formal reports / briefings / email / phone / meetings etc)
   Is it pre-assessed by others first?

9. Do you, or the organisation, use any criteria or system to evaluate or grade the quality of information and intelligence gathered, shared or received?
   You
   FACT
   Internally sourced / developed intelligence
   Externally sourced / developed intelligence
   Can it be relied upon?

INTELLIGENCE SHARING

10. Do you deal with other organisations in the operational work that you do – those with which FACT shares information or intelligence?
    To what extent?
    What is your involvement?
    How do you manage these relationships?
    Incoming intelligence - processes
    Outgoing intelligence - processes

11. From your experience, how well does intelligence sharing work at FACT?
    Why?

12. Are there any problems that you experience in intelligence sharing with other organisations?
    What are these?
    Any particularly good or bad organisations?
    Is there enough sharing?
    Technical issues
    Cultural Issues
    Political Issues

13. How would you rate the culture within FACT with respect to intelligence handling and sharing?
    Why?
    Any way it could be improved?

Restrictions

14. Do you or your place any restrictions or conditions upon the information and intelligence shared with partners, and are you able to outline these?
    Onward sharing of information and intelligence (within or outside of network)

15. Are there any circumstances in which you or the organisation would be unwilling to share information / intelligence with other parties?
    What are these?
    What would need to change in order to allow or enable sharing?

16. Are there any circumstances in which your team would be unwilling to receive or process information / intelligence from other parties?
    What are these?
    What would need to change in order to allow or enable sharing?

CASES

17. Would you be able to talk me through an example of a case, or cases, that you have worked on where intelligence or information sourced from partner organisations has played a role?
    Overview of the case and situation?
    How did it come to light?
    What was your role?
    How did information or intelligence play a part in the case?
    Where did the information or intelligence come from?
    How was it identified – (e.g. volunteered by partner or requested by FACT?)
    How was it used?
    Outcome of case?
    Feedback to partner organisation?

FINAL

18. Is there anything that you would like to see done to better facilitate effective information and intelligence sharing in future (with respect to FACT, or the UK in general)?
    Changes to legislation
    System of licensing for those who hold and share data
    Training/accreditation
    Other

19. Are you aware of any good practice or innovation in this area, in the UK or overseas, that could be utilised more widely in the UK?

20. Is there anything more that you would like to add that we have not addressed?

[Closure – thank you for your time and participation]

Interview Schedule: Human Resources

PREAMBLE: This interview is being conducted as part of case study research into information and intelligence sharing at the Federation Against Copyright Theft. The case study itself is part of a wider piece of doctoral research into anti-fraud information and intelligence sharing.

The interview is entirely voluntary, and your identity as a participant will not be disclosed in any output detailing the findings of the research. This interview is being recorded – please could you confirm that you consent to its being recorded? Thank you.

ABOUT YOUR ROLE

1. What is your job title?

2. Please could you give me an overview of your role within FACT?
   What do you do?
   How do you go about it?
   Typical day / Regular tasks
   Systems & Processes Used
   Output and production

ABOUT THE HR FUNCTION

3. What are the responsibilities within the HR function?

4. How do you ensure that FACT teams are getting the correct support?

5. How do you support the individual employees working for FACT?
   Guidance
   Training
   Processes

6. What qualities, experience and background do you tend to look for in recruiting staff?
   Investigation Staff
   Staff with intelligence handling responsibilities
   Staff whose role involves collaborating with other organisations

7. Are there specific procedural documents for staff on intelligence handling and sharing issues?
   Procedural documents
   Guidance manuals
   Training packages
   Is it possible to get copies of these documents?

8. Are there specific procedures in place for assessing how well staff are performing in handling and sharing intelligence?
   What are they?
   How do they work?
   Who performs them?

OTHER ASPECTS OF ROLE (E.G. FILM INDUSTRY LIAISON)

9. Please could you provide me with an overview of any additional elements of your work that are not necessarily related to HR?
   What do you do?
   Who do you deal with (internally / externally)?
   How do these relationships work?
   How does this fit in with FACT's purpose?

FINAL

10. Is there anything more that you would like to add that we have not addressed?

[Closure – thank you for your time and participation]

Interview Schedule: Intelligence Analyst

PREAMBLE: This interview is being conducted as part of case study research into information and intelligence sharing at the Federation Against Copyright Theft. The case study itself is part of a wider piece of doctoral research into anti-fraud information and intelligence sharing.

The interview is entirely voluntary, and your identity as a participant will not be disclosed in any output detailing the findings of the research. This interview is being recorded – please could you confirm that you consent to its being recorded? Thank you.

ABOUT YOUR ROLE

1. Please could you give me an overview of your role within FACT?
   What do you do?
   How do you go about it?
   Involvement in individual cases
   Involvement in establishing and maintaining relationships with partner organisations

ABOUT YOUR TEAM

2. Please could you give me a broad overview of your team and its work, in terms of what it does and what it aims to achieve?

3. How does the work that your team does fit in with the overall work of FACT?

4. How would you assess the role that intelligence and information plays within the way that FACT operates?
   Importance

INTELLIGENCE AND INFORMATION ANALYSIS AND USE

5. How do you use information and intelligence within your work?
   Daily basis
   Investigations / case work
   Other uses

6. How does your team operate in terms of the intelligence model (e.g. NIM) used by FACT?
   How is this translated into use?
   How does this serve the organisation?
   Benefits
   Drawbacks / problems

7. What does your role normally involve as an intelligence analyst?

8. How is the information or intelligence that you process received by you?
   Original source?
   How does it get to FACT?

How does it get onto your desk?

9. What systems and tools do you use to gather and develop information and intelligence?
   Online
   Offline
   How are they used?
   Production of intelligence products

10. What intelligence outputs and products do you, and your team, produce?
    How are these produced?
    How are these used in FACT's work?

11. Do you, or your team, produce any specific information or intelligence outputs or products for the partner organisations with which it has intelligence sharing arrangements?
    Are these ever produced solely for partners?
    Types of output / product
    Do they differ in content to what you produce for internal use?
    When are these produced (e.g. on request / when identified as relevant)
    How do you understand your partners' information or intelligence needs? (e.g. agreements, feedback processes)
    Who makes the decisions to share / is there an authorisation process?

12. Do you, or your team, receive any specific information or intelligence outputs or products from the partner organisations with which it has intelligence sharing arrangements?
    Are these ever produced solely for FACT?
    Types of output / product
    When are these produced (e.g. on request / when identified as relevant)
    How do your partners understand FACT's information or intelligence needs? (e.g. agreements, feedback processes)

13. Does your team approach, process or manage the information and intelligence received from partner organisations in a different way to that which it gathers and develops itself?
    How?
    Why?
    Are different approaches taken for different partner organisations? If so, why?

14. Are there different approaches or processes in place with respect to sharing either data, information or intelligence?
    [If yes] How do they differ?
    Why?
    What are the implications (if any) for your work, or the work of FACT and/or its partners?

15. How do you view how effectively the team gathers and utilises information and intelligence?
    Effective / Ineffective
    How do you rate it at the moment?
    How could it be improved?

RELATIONSHIPS WITH OTHER ORGANISATIONS

16. Are you involved in the management or maintenance of information or intelligence sharing relationships that FACT has with other organisations?
    [If yes] How are you involved?
    How do you approach information or intelligence sharing?
    Do the relationships work effectively in assisting you in your role?

17. How does FACT manage and maintain its relationships with its information sharing partners?
    Meetings
    Dedicated staff / points of contact
    Senior level relationships
    Process (formal or informal) to evaluate these relationships to ensure they're working

18. How do you or your team tend to provide or receive information and intelligence to and from partner organisations?
    Systems / phone / data packages / intelligence products etc

19. How is this usually managed from start (e.g. when information/intelligence is identified as being of potential interest) to finish (e.g. information/intelligence is used or discarded after processing and analysis).
    Individual steps
    How do organisations notify each other at start
    Agreement to share, formats etc
    Communication channel (secure?)
    Receipt / transmission
    Storage
    Processing steps
    Corroboration
    Analysis etc

20. Is feedback generally provided or sought in respect of information or intelligence shared between FACT and partner organisations?
    What type?
    When?
    Is this important, and how?

21. In your role as Intelligence Analyst, how effective do you find the information and intelligence sharing relationships that FACT has to be in sourcing good quality inputs that are relevant to FACT's mission?
    Does FACT have the right partners?
    Do they provide what FACT needs?
    Does FACT provide what they need?
    Are some partnerships better than others? Why?
    Are there any characteristics of partnership organisations that are better or worse than others (e.g. by sector, industry etc)
    Can you think of how these relationships can be improved further?

BARRIERS AND PROBLEMS TO INFORMATION SHARING

Technical

22. From your experience, what have been the most significant technical challenges that have impeded, or that have had to be tackled in respect of, sharing information or intelligence with other organisations?
    Data formats
    Data quality
    Data volume
    Other technical issues

23. How has FACT overcome these challenges?

24. Do any technical barriers still exist that impede, or sometimes prevent, effective information or intelligence sharing with other organisations?

Political / Legal

25. What have been the most significant political or legal challenges that have impeded, or that have had to be tackled in respect of, sharing information or intelligence with other organisations?
    Financial
    Political
    Bureaucratic
    Standards
    Legislative
    Cross-jurisdictional

26. How has FACT overcome these challenges?

27. Do any political or legal barriers still exist that impede, or sometimes prevent, effective information or intelligence sharing with other organisations?

Organisational / Cultural

28. What have been the most significant organisational or cultural challenges that have impeded, or that have had to be tackled in respect of, sharing information or intelligence with other organisations?
    Unwillingness to share
    Lack of trust
    Lack of feedback
    Ownership of information / intelligence
    Information asymmetry
    Non-reciprocal information flow
    Lack of understanding of partners' needs'

29. How has FACT overcome these challenges?

30. Do any organisational or cultural barriers still exist that impede, or sometimes prevent, effective information or intelligence sharing with other organisations?

Restrictions

31. Does FACT place any restrictions or conditions upon the information and intelligence shared with partners, and are you able to outline these?
    Onward sharing of information and intelligence (within or outside of network)

32. Are there any circumstances in which you or the organisation would be unwilling to share information / intelligence with other parties?
    What are these?
    What would need to change in order to allow or enable sharing?

33. Are there any circumstances in which you or your team would be unwilling to receive or process information / intelligence from other parties?
    What are these?
    What would need to change in order to allow or enable sharing?

FINAL

34. Is there anything that you would like to see done to better facilitate effective information and intelligence sharing in future in the UK (with respect to FACT, or the UK in general)?
    Changes to legislation
    System of licensing for those who hold and share data
    Training/accreditation

35. Are you aware of any good practice or innovation in this area, in the UK or overseas, that could be utilised more widely in the UK?

36. Is there anything more that you would like to add that we have not addressed?

[Closure – thank you for your time and participation]

Interview Schedule: Intelligence Manager

PREAMBLE: This interview is being conducted as part of case study research into information and intelligence sharing at the Federation Against Copyright Theft. The case study itself is part of a wider piece of doctoral research into anti-fraud information and intelligence sharing.

The interview is entirely voluntary, and your identity as a participant will not be disclosed in any output detailing the findings of the research. This interview is being recorded – please could you confirm that you consent to its being recorded? Thank you.

ABOUT YOUR ROLE

1. Please could you give me an overview of your role within FACT?
   What do you do?
   How do you go about it?
   How do you set objectives and priorities for your teams?
   Involvement in individual cases
   Involvement in establishing and maintaining relationships with partner organisations

ABOUT YOUR TEAM

2. Please could you give me a broad overview of your team and its work, in terms of what it does and what it aims to achieve?
   Criminal Justice Officer
   Forensic Examiners
   Intelligence Analysts
   Intelligence Researchers
   Other

3. How many members of staff are there within the team for which you have responsibility?
   Within each function/role

4. How does the work that your team does fit in with the overall work of FACT?

5. How would you assess the role that intelligence and information plays within the way that FACT operates?
   Importance

INTELLIGENCE AND INFORMATION ANALYSIS AND USE

6. Does FACT, or your team, have or use a formal or working definition for data, information or intelligence, or use any other distinction between them?
   What are these?

7. How does your team seek to use information and intelligence within its work?
   Daily basis
   Investigations / case work
   Other uses

8. How does your team use operate in terms of the intelligence model (e.g. NIM) used by FACT?
   How is this translated into use?
   How does this serve the organisation?
   Benefits
   Drawbacks / problems

9. How does your team, and FACT more widely, gather and develop information and intelligence?
   What for?
   Where from?
   Who does this?
   How do they do it?

10. Does FACT use any criteria or system to evaluate or grade the quality of information and intelligence gathered, shared or received?
    Internally developed
    Shared – incoming
    Shared - outgoing
    How does this process work?
    Any corroboration processes used?

11. What systems (hardware/software) do you use to manage, process and use information and intelligence?
    Intelligence Analysts
    Intelligence Researchers
    Other roles

12. What systems and tools do you use to gather and develop information and intelligence?
    Online
    Offline
    Production of intelligence products

13. What intelligence outputs and products does the team produce?
    How are these used in FACT's work?

14. Does your team, or FACT, produce any specific information or intelligence outputs or products for the partner organisations with which it has intelligence sharing arrangements?
    Are these ever produced solely for partners?
    Types of output / product
    Do they differ in content to what you produce for internal use?
    When are these produced (e.g. on request / when identified as relevant)
    How do you understand your partners' information or intelligence needs? (e.g. agreements, feedback processes)
    Who makes the decisions to share / is there an authorisation process?

15. Does your team, or FACT, receive any specific information or intelligence outputs or products from the partner organisations with which it has intelligence sharing arrangements?
    Are these ever produced solely for FACT?
    Types of output / product
    When are these produced (e.g. on request / when identified as relevant)
    How do your partners understand FACT's information or intelligence needs? (e.g. agreements, feedback processes)

16. Does your team approach, process or manage the information and intelligence received from partner organisations in a different way to that which it gathers and develops itself?
    How?
    Why?
    Are different approaches taken for different partner organisations? If so, why?

17. Are there different approaches or processes in place with respect to sharing either data, information or intelligence?
    [If yes] How does it differ?
    Why?
    What are the implications (if any) for your work, or the work of FACT and/or its partners?

18. How do you evaluate how effectively the team gathers and utilises information and intelligence?
    Formal process
    How
    Who
    How often
    How do you rate it at the moment?

RELATIONSHIPS WITH OTHER ORGANISATIONS

19. Would you be able to provide me with an overview of how your organisation shares information and/or intelligence with others for the prevention or investigation of IP theft or fraud?
    With whom does it share?
    How does it share?
    What does it share (e.g. raw data / information / intelligence / intelligence products)
    Does it work effectively?

20. How does FACT manage and maintain its relationships with its information sharing partners?
    Meetings
    Dedicated staff / points of contact
    Senior level relationships
    Process (formal or informal) to evaluate these relationships to ensure they're working

21. How does your team tend to provide or receive information and intelligence to and from partner organisations?
    Systems / phone / data packages / intelligence products etc

22. How is this usually managed from start (e.g. when information/intelligence is identified as being of potential interest) to finish (e.g. information/intelligence is used or discarded after processing and analysis).
    Individual steps
    How do organisations notify each other at start
    Agreement to share, formats etc
    Communication channel (secure?)
    Receipt / transmission
    Storage
    Processing steps
    Corroboration
    Analysis etc

23. Is feedback generally provided or sought in respect of information or intelligence shared between FACT and partner organisations?
    What type?
    When?
    Is this important, and how?

24. In your role as Intelligence Manager, how effective do you find the information and intelligence sharing relationships that FACT has to be in sourcing good quality inputs that are relevant to FACT's mission?
    Does FACT have the right partners?
    Do they provide what FACT needs?
    Does FACT provide what they need?
    Are some partnerships better than others? Why?
    Are there any characteristics of partnership organisations that are better or worse than others (e.g. by sector, industry etc)
    Can you think of how these relationships can be improved further?

BARRIERS AND PROBLEMS TO INFORMATION SHARING

Technical

25. From your experience and your team's perspective, what have been the most significant technical challenges that have impeded, or that have had to be tackled in respect of, sharing information or intelligence with other organisations?
    Data formats
    Data quality
    Data volume
    Other technical issues

26. How has FACT overcome these challenges?

27. Do any technical barriers still exist that impede, or sometimes prevent, effective information or intelligence sharing with other organisations?

Political / Legal

28. What have been the most significant political or legal challenges that have impeded, or that have had to be tackled in respect of, sharing information or intelligence with other organisations?
    Financial
    Political
    Bureaucratic
    Standards
    Legislative
    Cross-jurisdictional

29. How has FACT overcome these challenges?

30. Do any political or legal barriers still exist that impede, or sometimes prevent, effective information or intelligence sharing with other organisations?

Organisational / Cultural

31. What have been the most significant organisational or cultural challenges that have impeded, or that have had to be tackled in respect of, sharing information or intelligence with other organisations?
    Unwillingness to share
    Lack of trust
    Lack of feedback
    Ownership of information / intelligence
    Information asymmetry
    Non-reciprocal information flow
    Lack of understanding of partners' needs'

32. How has FACT overcome these challenges?

33. Do any organisational or cultural barriers still exist that impede, or sometimes prevent, effective information or intelligence sharing with other organisations?

Restrictions

34. Does your team place any restrictions or conditions upon the information and intelligence shared with partners, and are you able to outline these?
    Onward sharing of information and intelligence (within or outside of network)

35. Are there any circumstances in which you or the organisation would be unwilling to share information / intelligence with other parties?
    What are these?
    What would need to change in order to allow or enable sharing?

36. Are there any circumstances in which your team would be unwilling to receive or process information / intelligence from other parties?
    What are these?
    What would need to change in order to allow or enable sharing?

FINAL

37. Is there anything that you would like to see done to better facilitate effective information and intelligence sharing in future in the UK (with respect to FACT, or the UK in general)?
    Changes to legislation
    System of licensing for those who hold and share data
    Training/accreditation

38. Are you aware of any good practice or innovation in this area, in the UK or overseas, that could be utilised more widely in the UK?

39. Is there anything more that you would like to add that we have not addressed?

[Closure – thank you for your time and participation]

Interview Schedule: Intelligence Researcher

PREAMBLE: This interview is being conducted as part of case study research into information and intelligence sharing at the Federation Against Copyright Theft. The case study itself is part of a wider piece of doctoral research into anti-fraud information and intelligence sharing.

The interview is entirely voluntary, and your identity as a participant will not be disclosed in any output detailing the findings of the research. This interview is being recorded – please could you confirm that you consent to its being recorded? Thank you.

ABOUT YOUR ROLE

1. Please could you give me an overview of your role within FACT?
   What do you do?
   How do you go about it?
   Involvement in individual cases
   Involvement in establishing and maintaining relationships with partner organisations

ABOUT YOUR TEAM

2. Please could you give me a broad overview of your team and its work, in terms of what it does and what it aims to achieve?

3. How does the work that your team does fit in with the overall work of FACT?

4. How would you assess the role that intelligence and information plays within the way that FACT operates?
   Importance

INTELLIGENCE AND INFORMATION ANALYSIS AND USE

5. How do you use information and intelligence within your work?
   Daily basis
   Investigations / case work
   Other uses

6. How does your team operate in terms of the intelligence model (e.g. NIM) used by FACT?
   How is this translated into use?
   How does this serve the organisation?
   Benefits
   Drawbacks / problems

7. What does your role normally involve as an intelligence researcher?

8. How is the information or intelligence that you process received by you?
   Original source?
   How does it get to FACT?
   How does it get onto your desk?

9. What systems and tools do you use to research, gather and develop information and intelligence?
   Online
   Offline
   How are they used?
   Production of intelligence products

10. What intelligence outputs and products do you, and your team, produce?
    How are these produced?
    How are these used in FACT's work?

11. Do you, or your team, produce any specific information or intelligence outputs or products for the partner organisations with which it has intelligence sharing arrangements?
    Are these ever produced solely for partners?
    Types of output / product
    Do they differ in content to what you produce for internal use?
    When are these produced (e.g. on request / when identified as relevant)
    How do you understand your partners' information or intelligence needs? (e.g. agreements, feedback processes)
    Who makes the decisions to share / is there an authorisation process?

12. Do you, or your team, receive any specific information or intelligence outputs or products from the partner organisations with which it has intelligence sharing arrangements?
    Are these ever produced solely for FACT?
    Types of output / product
    When are these produced (e.g. on request / when identified as relevant)
    How do your partners understand FACT's information or intelligence needs? (e.g. agreements, feedback processes)

13. Does your team approach, process or manage the information and intelligence received from partner organisations in a different way to that which it gathers and develops itself?
    How?
    Why?
    Are different approaches taken for different partner organisations? If so, why?

14. Are there different approaches or processes in place with respect to sharing either data, information or intelligence?
    [If yes] How does it differ?
    Why?
    What are the implications (if any) for your work, or the work of FACT and/or its partners?

15. How do you view how effectively the team gathers and utilises information and intelligence?
    Effective / Ineffective
    How do you rate it at the moment?
    How could it be improved?

RELATIONSHIPS WITH OTHER ORGANISATIONS

16. Are you involved in the management or maintenance of information or intelligence sharing relationships that FACT has with other organisations?
    [If yes] How are you involved?
    How do you approach information or intelligence sharing?
    Do the relationships work effectively in assisting you in your role?

17. How does FACT manage and maintain its relationships with its information sharing partners?
    Meetings
    Dedicated staff / points of contact
    Senior level relationships
    Process (formal or informal) to evaluate these relationships to ensure they're working

18. How do you or your team tend to provide or receive information and intelligence to and from partner organisations?
    Systems / phone / data packages / intelligence products etc

19. How is this usually managed from start (e.g. when information/intelligence is identified as being of potential interest) to finish (e.g. information/intelligence is used or discarded after processing and analysis).
    Individual steps
    How do organisations notify each other at start
    Agreement to share, formats etc
    Communication channel (secure?)
    Receipt / transmission
    Storage
    Processing steps
    Corroboration
    Analysis etc

20. Is feedback generally provided or sought in respect of information or intelligence shared between FACT and partner organisations?
    What type?
    When?
    Is this important, and how?

21. In your role as Intelligence Researcher, how effective do you find the information and intelligence sharing relationships that FACT has to be in sourcing good quality inputs that are relevant to FACT's mission?
    Does FACT have the right partners?
    Do they provide what FACT needs?
    Does FACT provide what they need?
    Are some partnerships better than others? Why?
    Are there any characteristics of partnership organisations that are better or worse than others (e.g. by sector, industry etc)
    Can you think of how these relationships can be improved further?

BARRIERS AND PROBLEMS TO INFORMATION SHARING

Technical

22. From your experience, what have been the most significant technical challenges that have impeded, or that have had to be tackled in respect of, sharing information or intelligence with other organisations?
    Data formats
    Data quality
    Data volume
    Other technical issues

23. How has FACT overcome these challenges?

24. Do any technical barriers still exist that impede, or sometimes prevent, effective information or intelligence sharing with other organisations?

Political / Legal

25. What have been the most significant political or legal challenges that have impeded, or that have had to be tackled in respect of, sharing information or intelligence with other organisations?
    Financial
    Political
    Bureaucratic
    Standards
    Legislative
    Cross-jurisdictional

26. How has FACT overcome these challenges?

27. Do any political or legal barriers still exist that impede, or sometimes prevent, effective information or intelligence sharing with other organisations?

Organisational / Cultural

28. What have been the most significant organisational or cultural challenges that have impeded, or that have had to be tackled in respect of, sharing information or intelligence with other organisations?
    Unwillingness to share
    Lack of trust
    Lack of feedback
    Ownership of information / intelligence
    Information asymmetry
    Non-reciprocal information flow
    Lack of understanding of partners' needs'

29. How has FACT overcome these challenges?

30. Do any organisational or cultural barriers still exist that impede, or sometimes prevent, effective information or intelligence sharing with other organisations?

Restrictions

31. Does FACT place any restrictions or conditions upon the information and intelligence shared with partners, and are you able to outline these?
    Onward sharing of information and intelligence (within or outside of network)

32. Are there any circumstances in which you or the organisation would be unwilling to share information / intelligence with other parties?
    What are these?
    What would need to change in order to allow or enable sharing?

33. Are there any circumstances in which you or your team would be unwilling to receive or process information / intelligence from other parties?
    What are these?
    What would need to change in order to allow or enable sharing?

FINAL

34. Is there anything that you would like to see done to better facilitate effective information and intelligence sharing in future in the UK (with respect to FACT, or the UK in general)?
    Changes to legislation
    System of licensing for those who hold and share data
    Training/accreditation

35. Are you aware of any good practice or innovation in this area, in the UK or overseas, that could be utilised more widely in the UK?

36. Is there anything more that you would like to add that we have not addressed?

[Closure – thank you for your time and participation]

Interview Schedule: Internet Investigator

PREAMBLE: This interview is being conducted as part of case study research into information and intelligence sharing at the Federation Against Copyright Theft. The case study itself is part of a wider piece of doctoral research into anti-fraud information and intelligence sharing.

The interview is entirely voluntary, and your identity as a participant will not be disclosed in any output detailing the findings of the research. This interview is being recorded – please could you confirm that you consent to its being recorded? Thank you.

ABOUT YOUR ROLE

1. What is your job title?

2. Please could you give me an overview of your role within FACT?
   What do you do?
   How do you go about it?
   Typical day / Regular tasks
   Output and production

3. How do you go about internet investigation?
   Methods
   Processes
   Systems
   Sites
   Open Source Intelligence
   Assessing Quality
   Rules and restrictions
   How do you ensure that evidence gathered online is usable in cases and court?

4. How do you keep up to date on techniques and online resources?
   Training
   Finding resources and sites
   Assessing resources and sites

ABOUT YOUR TEAM

5. How does your role fit in with the rest of your team?
   Working with others (vertically / horizontally)
   Interaction / Communication
   How is team organised?

6. How are your working goals and objectives set?
   How set, and who by?
   How are they measured?

7. How does the work that your team does fit in with the overall work of FACT?
   Goals
   Case work
   Interaction (working together)
   Formal / informal channels or processes for working with other teams?

8. How would you assess the role that intelligence and information plays within the way that FACT operates?
   Importance
   Open Source Intelligence
   Shared Intelligence

INTELLIGENCE AND INFORMATION ANALYSIS AND USE

9. How do you use information and intelligence within your work?
   Daily basis
   Investigations / case work
   Other uses

10. How does intelligence and information that you use in your work reach you?
    Where from (internally / externally)?
    In what forms does it reach you (formal reports / briefings / email / phone / meetings etc)
    Is it pre-assessed by others first?

11. Do you, or the organisation, use any criteria or system to evaluate or grade the quality of information and intelligence gathered, shared or received?
    You
    FACT
    Internally sourced / developed intelligence
    Externally sourced / developed intelligence
    Can it be relied upon?

INTELLIGENCE SHARING

12. Do you deal with other organisations in the operational work that you do – those with which FACT shares information or intelligence?
    To what extent?
    What is your involvement?
    How do you manage these relationships?
    Incoming intelligence - processes
    Outgoing intelligence - processes

13. From your experience, how well does intelligence sharing work at FACT?
    Why?

14. Are there any problems that you experience in intelligence sharing with other organisations?
    What are these?
    Any particularly good or bad organisations?
    Is there enough sharing?
    Technical issues (inc. quality of info)
    Cultural Issues
    Political Issues

15. How would you rate the culture within FACT with respect to intelligence handling and sharing?
    Why?
    Any way it could be improved?

Restrictions

16. Do you or your place any restrictions or conditions upon the information and intelligence shared with partners, and are you able to outline these?
    Onward sharing of information and intelligence (within or outside of network)

17. Are there any circumstances in which you or the organisation would be unwilling to share information / intelligence with other parties?
    What are these?
    What would need to change in order to allow or enable sharing?

18. Are there any circumstances in which your team would be unwilling to receive or process information / intelligence from other parties?
    What are these?
    What would need to change in order to allow or enable sharing?

CASES

19. Would you be able to talk me through an example of a case, or cases, that you have worked on where intelligence or information sourced from partner organisations has played a role?
    Overview of the case and situation?
    How did it come to light?
    What was your role?
    How did information or intelligence play a part in the case?
    Where did the information or intelligence come from?
    How was it identified – (e.g. volunteered by partner or requested by FACT?)
    How was it used?
    Outcome of case?
    Feedback to partner organisation?

FINAL

20. Is there anything that you would like to see done to better facilitate effective information and intelligence sharing in future (with respect to FACT, or the UK in general)?
    Changes to legislation
    System of licensing for those who hold and share data
    Training/accreditation
    Other

21. Are you aware of any good practice or innovation in this area, in the UK or overseas, that could be utilised more widely in the UK?

22. Is there anything more that you would like to add that we have not addressed?

[Closure – thank you for your time and participation]

Interview Schedule: Internet Researcher

PREAMBLE: This interview is being conducted as part of case study research into information and intelligence sharing at the Federation Against Copyright Theft. The case study itself is part of a wider piece of doctoral research into anti-fraud information and intelligence sharing.

The interview is entirely voluntary, and your identity as a participant will not be disclosed in any output detailing the findings of the research. This interview is being recorded – please could you confirm that you consent to its being recorded? Thank you.

ABOUT YOUR ROLE

1. What is your job title?

2. Please could you give me an overview of your role within FACT?
   What do you do?
   How do you go about it?
   Typical day / Regular tasks
   Output and production

3. How do you go about internet research?
   Methods
   Processes
   Systems
   Sites
   Assessing Quality
   Rules and restrictions
   How do you ensure that evidence gathered online is usable in cases and court?

4. How do you keep up to date on techniques and online resources?
   Training
   Finding resources and sites
   Assessing resources and sites

ABOUT YOUR TEAM

5. How does your role fit in with the rest of your team?
   Working with others (vertically / horizontally)
   Interaction / Communication
   How is team organised?

6. How are your working goals and objectives set?
   How set, and who by?
   How are they measured?

7. How does the work that your team does fit in with the overall work of FACT?
   Goals
   Case work
   Interaction (working together)
   Formal / informal channels or processes for working with other teams?

8. How would you assess the role that intelligence and information plays within the way that FACT operates?
   Importance
   Open Source Intelligence
   Shared Intelligence

INTELLIGENCE AND INFORMATION ANALYSIS AND USE

9. How do you use information and intelligence within your work?
   Daily basis
   Investigations / case work
   Other uses

10. How does intelligence and information that you use in your work reach you?
    Where from (internally / externally)?
    In what forms does it reach you (formal reports / briefings / email / phone / meetings etc)
    Is it pre-assessed by others first?

11. Do you, or the organisation, use any criteria or system to evaluate or grade the quality of information and intelligence gathered, shared or received?
    You
    FACT
    Internally sourced / developed intelligence
    Externally sourced / developed intelligence
    Can it be relied upon?

INTELLIGENCE SHARING

12. Do you deal with other organisations in the operational work that you do – those with which FACT shares information or intelligence?
    To what extent?
    What is your involvement?
    How do you manage these relationships?
    Incoming intelligence - processes
    Outgoing intelligence - processes

13. From your experience, how well does intelligence sharing work at FACT?
    Why?

14. Are there any problems that you experience in intelligence sharing with other organisations?
    What are these?
    Any particularly good or bad organisations?
    Is there enough sharing?
    Technical issues
    Cultural Issues
    Political Issues

15. How would you rate the culture within FACT with respect to intelligence handling and sharing?
    Why?
    Any way it could be improved?

Restrictions

16. Do you or your place any restrictions or conditions upon the information and intelligence shared with partners, and are you able to outline these?
    Onward sharing of information and intelligence (within or outside of network)

17. Are there any circumstances in which you or the organisation would be unwilling to share information / intelligence with other parties?
    What are these?
    What would need to change in order to allow or enable sharing?

18. Are there any circumstances in which your team would be unwilling to receive or process information / intelligence from other parties?
    What are these?
    What would need to change in order to allow or enable sharing?

CASES

19. Would you be able to talk me through an example of a case, or cases, that you have worked on where intelligence or information sourced from partner organisations has played a role?
    Overview of the case and situation?
    How did it come to light?
    What was your role?
    How did information or intelligence play a part in the case?
    Where did the information or intelligence come from?
    How was it identified – (e.g. volunteered by partner or requested by FACT?)
    How was it used?
    Outcome of case?
    Feedback to partner organisation?

FINAL

20. Is there anything that you would like to see done to better facilitate effective information and intelligence sharing in future (with respect to FACT, or the UK in general)?
    Changes to legislation
    System of licensing for those who hold and share data
    Training/accreditation
    Other

21. Are you aware of any good practice or innovation in this area, in the UK or overseas, that could be utilised more widely in the UK?

22. Is there anything more that you would like to add that we have not addressed?

[Closure – thank you for your time and participation]

Interview Schedule: Internet Supervisor

PREAMBLE: This interview is being conducted as part of case study research into information and intelligence sharing at the Federation Against Copyright Theft. The case study itself is part of a wider piece of doctoral research into anti-fraud information and intelligence sharing.

The interview is entirely voluntary, and your identity as a participant will not be disclosed in any output detailing the findings of the research. This interview is being recorded – please could you confirm that you consent to its being recorded? Thank you.

ABOUT YOUR ROLE AND YOUR TEAM

1. What is your job title?

2. Please could you give me an overview of your role within FACT?
   What do you do?
   How do you go about it?
   How do you set objectives and priorities for your team?
   Involvement in individual cases
   Involvement in establishing and maintaining relationships with partner organisations

3. Please could you give me a broad overview of your team and its work, in terms of what it does and what it aims to achieve?
   Internet Investigators
   Systems Programmer

4. How many members of staff are there within the team for which you have responsibility?
   Within each function/role
   How is the team organised?

5. How does the work that your team does fit in with the overall work of FACT?

6. How would you assess the role that intelligence and information plays within the way that FACT operates?
   Importance
   Open Source Intelligence
   Shared Intelligence

7. How do you go about internet investigation?
   Methods
   Processes
   Systems
   Sites
   Open Source Intelligence
   Assessing Quality
   Rules and restrictions
   How do you ensure that evidence gathered online is usable in cases and court?

8. How do you keep yourself and your team up to date on techniques and online resources?
   Training
   Finding resources and sites
   Assessing resources and sites

INTELLIGENCE AND INFORMATION ANALYSIS AND USE

9. How do you use information and intelligence within your work?
   Daily basis
   Investigations / case work
   Other uses

10. How does intelligence and information that you use in your work reach you?
    Where from (internally / externally)?
    In what forms does it reach you (formal reports / briefings / email / phone / meetings etc)
    Is it pre-assessed by others first?

11. Do you, or the organisation, use any criteria or system to evaluate or grade the quality of information and intelligence gathered, shared or received?
    You
    FACT
    Internally sourced / developed intelligence
    Externally sourced / developed intelligence
    Can it be relied upon?

INTELLIGENCE SHARING

12. Do you deal with other organisations in the operational work that you do – those with which FACT shares information or intelligence?
    To what extent?
    What is your involvement?
    How do you manage these relationships?
    Incoming intelligence - processes
    Outgoing intelligence - processes

13. From your experience, how well does intelligence sharing work at FACT?
    Why?

14. Are there any problems that you experience in intelligence sharing with other organisations?
    What are these?
    Any particularly good or bad organisations?
    Is there enough sharing?
    Technical issues
    Cultural Issues
    Political Issues

15. How would you rate the culture within FACT with respect to intelligence handling and sharing?
    Why?
    Any way it could be improved?

Restrictions

16. Do you or your place any restrictions or conditions upon the information and intelligence shared with partners, and are you able to outline these?
    Onward sharing of information and intelligence (within or outside of network)

17. Are there any circumstances in which you or the organisation would be unwilling to share information / intelligence with other parties?
    What are these?
    What would need to change in order to allow or enable sharing?

18. Are there any circumstances in which your team would be unwilling to receive or process information / intelligence from other parties?
    What are these?
    What would need to change in order to allow or enable sharing?

CASES

19. Would you be able to talk me through an example of a case, or cases, that you have worked on where intelligence or information sourced from partner organisations has played a role?
    Overview of the case and situation?
    How did it come to light?
    What was your role?
    How did information or intelligence play a part in the case?
    Where did the information or intelligence come from?
    How was it identified – (e.g. volunteered by partner or requested by FACT?)
    How was it used?
    Outcome of case?
    Feedback to partner organisation?

FINAL

20. Is there anything that you would like to see done to better facilitate effective information and intelligence sharing in future (with respect to FACT, or the UK in general)?
    Changes to legislation
    System of licensing for those who hold and share data
    Training/accreditation
    Other

21. Are you aware of any good practice or innovation in this area, in the UK or overseas, that could be utilised more widely in the UK?

22. Is there anything more that you would like to add that we have not addressed?

[Closure – thank you for your time and participation]

Interview Schedule: Investigations Manager

PREAMBLE: This interview is being conducted as part of case study research into information and intelligence sharing at the Federation Against Copyright Theft. The case study itself is part of a wider piece of doctoral research into anti-fraud information and intelligence sharing.

The interview is entirely voluntary, and your identity as a participant will not be disclosed in any output detailing the findings of the research. This interview is being recorded – please could you confirm that you consent to its being recorded? Thank you.

ABOUT YOUR ROLE

1. Please could you give me an overview of your role within FACT?
   What do you do?
   How do you go about it?
   How do you set objectives and priorities for your teams?
   Involvement in individual cases
   Involvement in establishing and maintaining relationships with partner organisations

ABOUT YOUR TEAM

2. Please could you give me a broad overview of your teams and their work, in terms of what it does and what it aims to achieve?
   Field investigations
   Internet investigations

3. How many members of staff are there within the teams for which you have responsibility?
   Within each function/role

4. How does the work that your teams do fit in with the overall work of FACT?

5. How would you assess the role that intelligence and information plays within the way that FACT operates?
   Relevance
   Importance

INTELLIGENCE AND INFORMATION ANALYSIS AND USE

6. Does FACT, or your team, have or use a formal or working definition for data, information or intelligence, or use any other distinction between them?
   What are these?

7. How does your team seek to use information and intelligence within its work?
   Daily basis
   Investigations / case work
   Other uses

8. How does your team use operate in terms of the intelligence model (e.g. NIM) used by FACT?
   How is this translated into use?
   How does this serve the organisation?
   Benefits
   Drawbacks / problems

9. How does your team, and FACT more widely, gather and develop information and intelligence?
   What for?
   Where from?
   Who does this?
   How do they do it?

10. Does FACT use any criteria or system to evaluate or grade the quality of information and intelligence gathered, shared or received?
    Internally developed
    Shared – incoming
    Shared - outgoing
    How does this process work?
    Any corroboration processes used?

11. What systems (hardware/software) do you use to manage, process and use information and intelligence?
    Field investigators
    Internet investigators
    Others

12. What systems and tools do you use to gather and develop information and intelligence?
    Online
    Offline

13. What information or intelligence outputs and products does the team produce?
    How are these produced?
    How are these used in FACT's work?

14. Does your team, produce any specific information or intelligence outputs or products for the partner organisations with which it has intelligence sharing arrangements?
    Are these ever produced solely for partners?
    Types of output / product
    Do they differ in content to what you produce for internal use?
    When are these produced (e.g. on request / when identified as relevant)
    How do you understand your partners' information or intelligence needs? (e.g. agreements, feedback processes)
    Who makes the decisions to share / is there an authorisation process?

15. Does your team, or FACT, receive any specific information or intelligence outputs or products from the partner organisations with which it has intelligence sharing arrangements?
    Are these ever produced solely for FACT?
    Types of output / product
    When are these produced (e.g. on request / when identified as relevant)
    How do your partners understand FACT's information or intelligence needs? (e.g. agreements, feedback processes)

16. Does your team approach, process or manage the information and intelligence received from partner organisations in a different way to that which it gathers and develops itself?
    How?
    Why?
    Are different approaches taken for different partner organisations? If so, why?

17. Are there different approaches or processes in place with respect to sharing either data, information or intelligence?
    [If yes] How does it differ?
    Why?
    What are the implications (if any) for your work, or the work of FACT and/or its partners?

18. How do you evaluate how effectively the team gathers and utilises information and intelligence?
    Formal process
    How
    Who
    How often
    How do you rate it at the moment?

RELATIONSHIPS WITH OTHER ORGANISATIONS

19. How does your team tend to provide or receive information and intelligence to and from partner organisations?
    Systems / phone / data packages / intelligence products etc

20. How is this usually managed from start (e.g. when information/intelligence is identified as being of potential interest) to finish (e.g. information/intelligence is used or discarded after processing and analysis).
    Individual steps
    How do organisations notify each other at start
    Agreement to share, formats etc
    Communication channel (secure?)
    Receipt / transmission
    Storage
    Processing steps
    Corroboration
    Analysis etc

21. Is feedback generally provided or sought in respect of information or intelligence shared between FACT and partner organisations?
    What type?
    When?
    Is this important, and how?

22. In your role as Investigations Manager, how effective do you find the information and intelligence sharing relationships that FACT has to be in sourcing good quality inputs that are relevant to FACT's mission?
    Does FACT have the right partners?
    Do they provide what FACT needs?
    Does FACT provide what they need?
    Are some partnerships better than others? Why?
    Are there any characteristics of partnership organisations that are better or worse than others (e.g. by sector, industry etc)
    Can you think of how these relationships can be improved further?

BARRIERS AND PROBLEMS TO INFORMATION SHARING

Technical

23. From your experience and your team's perspective, what have been the most significant technical challenges that have impeded, or that have had to be tackled in respect of, sharing information or intelligence with other organisations?
    Data formats
    Data quality
    Data volume
    Other technical issues

24. How has FACT overcome these challenges?

25. Do any technical barriers still exist that impede, or sometimes prevent, effective information or intelligence sharing with other organisations?

Political / Legal

26. What have been the most significant political or legal challenges that have impeded, or that have had to be tackled in respect of, sharing information or intelligence with other organisations?
    Financial
    Political
    Bureaucratic
    Standards
    Legislative
    Cross-jurisdictional

27. How has FACT overcome these challenges?

28. Do any political or legal barriers still exist that impede, or sometimes prevent, effective information or intelligence sharing with other organisations?

Organisational / Cultural

29. What have been the most significant organisational or cultural challenges that have impeded, or that have had to be tackled in respect of, sharing information or intelligence with other organisations?
    Unwillingness to share
    Lack of trust
    Lack of feedback
    Ownership of information / intelligence
    Information asymmetry
    Non-reciprocal information flow
    Lack of understanding of partners' needs'

30. How has FACT overcome these challenges?

31. Do any organisational or cultural barriers still exist that impede, or sometimes prevent, effective information or intelligence sharing with other organisations?

Restrictions

32. Does your team place any restrictions or conditions upon the information and intelligence shared with partners, and are you able to outline these?
    Onward sharing of information and intelligence (within or outside of network)

33. Are there any circumstances in which you or the organisation would be unwilling to share information / intelligence with other parties?
    What are these?
    What would need to change in order to allow or enable sharing?

34. Are there any circumstances in which your team would be unwilling to receive or process information / intelligence from other parties?
    What are these?
    What would need to change in order to allow or enable sharing?

FINAL

35. Is there anything that you would like to see done to better facilitate effective information and intelligence sharing in future in the UK (with respect to FACT, or the UK in general)?
    Changes to legislation
    System of licensing for those who hold and share data
    Training/accreditation

36. Are you aware of any good practice or innovation in this area, in the UK or overseas, that could be utilised more widely in the UK?

37. Is there anything more that you would like to add that we have not addressed?

[Closure – thank you for your time and participation]

Interview Schedule: ISP Liaison

PREAMBLE: This interview is being conducted as part of case study research into information and intelligence sharing at the Federation Against Copyright Theft. The case study itself is part of a wider piece of doctoral research into anti-fraud information and intelligence sharing.

The interview is entirely voluntary, and your identity as a participant will not be disclosed in any output detailing the findings of the research. This interview is being recorded – please could you confirm that you consent to its being recorded? Thank you.

ABOUT YOUR ROLE

1. What is your job title?

2. Please could you give me an overview of your role within FACT?
   What do you do?
   How do you go about it?
   What types of organisations do you work with? How many?
   Typical day / Regular tasks
   Systems & Processes Used
   Output and production

3. How are your working goals and objectives set?
   How set, and who by?
   How are they measured?

4. How does the work that you do fit in with the overall work of FACT?
   Goals
   Case work
   Interaction (working together)
   Formal / informal channels or processes for working with other teams?

5. How would you assess the role that intelligence and information plays within the way that FACT operates?
   Importance

6. In what ways do you interact with ISPs and other organisations?
   What sort of relationships do you have with them?
   Co-operative?
   What factors influence relationships? (e.g. location, jurisdiction etc)
   Any problems or challenges in dealing with them?
   Do they ever provide information or intelligence?
   Does FACT ever provide them with information or intelligence?

INTELLIGENCE AND INFORMATION ANALYSIS AND USE

7. How do you use information and intelligence within your work?
   Daily basis
   Investigations / case work
   Other uses

8. How does intelligence and information that you use in your work reach you?
   Where from (internally / externally)?
   In what forms does it reach you (formal reports / briefings / email / phone / meetings etc)
   Is it pre-assessed by others first?

9. Do you, or the organisation, use any criteria or system to evaluate or grade the quality of information and intelligence gathered, shared or received?
   You
   FACT
   Internally sourced / developed intelligence
   Externally sourced / developed intelligence
   Can it be relied upon?

INTELLIGENCE SHARING

10. Do you deal with other organisations (i.e. non-ISPs) in the operational work that you do – those with which FACT shares information or intelligence?
    To what extent?
    What is your involvement?
    How do you manage these relationships?
    Incoming intelligence - processes
    Outgoing intelligence - processes

11. From your experience, how well does intelligence sharing work at FACT?
    Why?

12. Are there any problems that you experience in intelligence sharing with other organisations?
    What are these?
    Any particularly good or bad organisations?
    Is there enough sharing?
    Technical issues
    Cultural Issues
    Political Issues

13. How would you rate the culture within FACT with respect to intelligence handling and sharing?
    Why?
    Any way it could be improved?

Restrictions

14. Do you place any restrictions or conditions upon the information and intelligence shared with partners, and are you able to outline these?
    Onward sharing of information and intelligence (within or outside of network)

15. Are there any circumstances in which you or the organisation would be unwilling to share information / intelligence with other parties?
    What are these?
    What would need to change in order to allow or enable sharing?

16. Are there any circumstances in which your team would be unwilling to receive or process information / intelligence from other parties?
    What are these?
    What would need to change in order to allow or enable sharing?

CASES

17. Would you be able to talk me through an example of a case, or cases, that you have worked on where intelligence or information sourced from partner organisations has played a role?
    Overview of the case and situation?
    How did it come to light?
    What was your role?
    How did information or intelligence play a part in the case?
    Where did the information or intelligence come from?
    How was it identified – (e.g. volunteered by partner or requested by FACT?)
    How was it used?
    Outcome of case?
    Feedback to partner organisation?

FINAL

18. Is there anything that you would like to see done to better facilitate effective information and intelligence sharing in future (with respect to FACT, or the UK in general)?
    Changes to legislation
    System of licensing for those who hold and share data
    Training/accreditation
    Other

19. Are you aware of any good practice or innovation in this area, in the UK or overseas, that could be utilised more widely in the UK?

20. Is there anything more that you would like to add that we have not addressed?

[Closure – thank you for your time and participation]

Interview Schedule: IT Support

PREAMBLE: This interview is being conducted as part of case study research into information and intelligence sharing at the Federation Against Copyright Theft. The case study itself is part of a wider piece of doctoral research into anti-fraud information and intelligence sharing.

The interview is entirely voluntary, and your identity as a participant will not be disclosed in any output detailing the findings of the research. This interview is being recorded – please could you confirm that you consent to its being recorded? Thank you.

ABOUT YOUR ROLE

22. What is your job title?

23. Are you directly employed by FACT or by another organisation?

24. Please could you give me an overview of your role?
    What do you do?
    How do you go about it?
    Typical day / Regular tasks
    Output and production

ABOUT THE HR FUNCTION

25. What are the responsibilities within the IT Support function?

26. How do you ensure that FACT teams are getting the correct support?

27. How do you support the individual employees working for FACT?
    Guidance
    Training
    Processes

28. What types of systems (hardware and tools) do you supply and maintain for FACT?
    Office-based
    Mobile
    Remote working

29. What types of software do you source and supply for FACT?
    General software
    Specialist software (e.g. case management, investigation support, intelligence handling)
    What does the intelligence team use?
    What do the field investigators use?
    What do the internet investigators use?

30. How are IT and technology needs at FACT assessed?
    New IT
    Updates

Interim review
Budgetary constraints
What is the process for making requests for hardware and software?

31. How often is hardware and software replaced or updated?

32. How is the data collected, used and stored by FACT managed?
    Secure / encrypted
    Server based / cloud based
    Access control
    User access levels
    Password procedures

33. Is there any security protection or procedures relating to electronic communications, such as email?
    Encryption, etc?
    Restrictions on sending files, etc?

34. Do you provide any other support or services to FACT?

FINAL

1. Is there anything more that you would like to add that we have not addressed?

[Closure – thank you for your time and participation]

Interview Schedule: Legal Counsel

PREAMBLE: This interview is being conducted as part of case study research into information and intelligence sharing at the Federation Against Copyright Theft. The case study itself is part of a wider piece of doctoral research into anti-fraud information and intelligence sharing.

The interview is entirely voluntary, and your identity as a participant will not be disclosed in any output detailing the findings of the research. This interview is being recorded – please could you confirm that you consent to its being recorded? Thank you.

ABOUT YOUR ROLE

1. Please could you give me an overview of your own role within the organisation?
   What do you do?
   How do you go about it?
   Involvement in individual cases
   Involvement in establishing and maintaining relationships with partner organisations

LEGISLATIVE ENVIRONMENT RE INFORMATION & INTELLIGENCE

2. What are your views on the broad legal / legislative environment in which FACT operates in respect of its collection and usage of information and intelligence?
   Is it broadly helpful or unhelpful in respect of FACT's mission?
   Most helpful aspects?
   Most challenging aspects?

3. What legal channels does FACT utilise or attempt to utilise in order to assist it in gathering, using and sharing information?
   Which work well?
   Which do not work well?

4. What, in your view, are the greatest strengths of the current legislative environment and legal channels for FACT in terms of its gathering, usage and sharing of information and intelligence?
   UK
   Overseas

5. What, in your view, are the greatest weaknesses or shortcomings of the current legislative environment and legal channels for FACT in terms of its gathering, usage and sharing of information and intelligence?
   UK
   Overseas

6. How have you found the Data Protection legislation has affected FACT's work in respect of gathering and sharing information and intelligence?
   Enabler or barrier
   Well or poorly designed
   Interpretation by FACT
   Interpretation by other parties

7. Are there any other notable legal issues that affect FACT's handling and sharing of information and intelligence?
   What are these?
   Are there differences in respect of intelligence / information / data?
   How does FACT respond to these challenges?

RELATIONSHIPS WITH OTHER ORGANISATIONS

8. Are you involved in the process of drawing up or negotiating information and intelligence sharing agreements with other organisations?

9. [If yes] Please could you provide an overview of the process that is followed to establish these?
   Legal basis
   What legal issues need to be covered within the agreements?
   Are specific legal channels noted within the agreements?
   Are agreements reached over interpretation of specific legislation (so proceeding on mutual understanding)?
   Complicating factors / challenges

10. [If No] Why is your input as the legal counsel not required in the process for establishing information and intelligence sharing agreements and relationships?

11. What documentation is usually produced formalising information or intelligence sharing?

12. How often are the agreements reviewed / updated from a legal perspective, or otherwise requiring your input?

BARRIERS AND PROBLEMS TO INFORMATION SHARING

Political / Legal

13. In your view, what are the most significant issues that impede and have to be tackled in respect of sharing information and intelligence with other organisations?
   Political/Legal
   Organisational/cultural
   Technical

14. How has FACT overcome these challenges?

15. Do any barriers still exist that impede, or sometimes prevent, effective information or intelligence sharing with other organisations?

16. How do cross-jurisdictional issues affect the legal processes that FACT must follow in pursuing its goals
   Generally
   Information and intelligence sharing

17. How does the increasingly online nature of IP theft/fraud affect the approach that FACT takes to information / intelligence handling and sharing from a legal perspective?
    National / international law on criminality
    Cross-jurisdictional issues re info sharing
    Defining where criminal offences take place

Restrictions

18. Does FACT place any restrictions or conditions upon the information and intelligence shared with partners, and are you able to outline these?
    Suspected/confirmed fraud
    Onward sharing of information and intelligence (within or outside of network)

19. Are there any circumstances in which you would advise FACT against sharing information / intelligence with other parties?
    What are these?
    What would need to change in order to allow or enable sharing?

FINAL

20. Is there anything that you would like to see done to better facilitate effective information and intelligence sharing in future in the UK?
    Changes to legislation

21. Are you aware of any good practice or innovation in this area, in the UK or overseas, that could be utilised more widely in the UK?

22. Is there anything more that you would like to add that we have not addressed?

[Closure – thank you for your time and participation]

Interview Schedule: Market Strategist

PREAMBLE: This interview is being conducted as part of case study research into information and intelligence sharing at the Federation Against Copyright Theft. The case study itself is part of a wider piece of doctoral research into anti-fraud information and intelligence sharing.

The interview is entirely voluntary, and your identity as a participant will not be disclosed in any output detailing the findings of the research. This interview is being recorded – please could you confirm that you consent to its being recorded? Thank you.

ABOUT YOUR ROLE

1. What is your job title?

2. Please could you give me an overview of your role within FACT?
   What do you do?
   How do you go about it?
   What types of organisations do you work with? How many?
   Typical day / Regular tasks
   Systems & Processes Used
   Output and production

3. How are your working goals and objectives set?
   How set, and who by?
   How are they measured?

4. How does the work that you do fit in with the overall work of FACT?
   Goals
   Case work
   Interaction (working together)
   Formal / informal channels or processes for working with other teams?

5. How would you assess the role that intelligence and information plays within the way that FACT operates?
   Importance

6. In what ways do you interact with other organisations?
   What sort of relationships do you have with them?
   Co-operative?
   What factors influence relationships? (e.g. location, jurisdiction etc)
   How are the relationships managed?
   Any problems or challenges in dealing with them?
   Do they ever provide information or intelligence?
   Does FACT ever provide them with information or intelligence?

INTELLIGENCE AND INFORMATION ANALYSIS AND USE [IF RELEVANT]

7. How do you use information and intelligence within your work?
   Daily basis
   Investigations / case work
   Other uses

8. How does intelligence and information that you use in your work reach you?
   Where from (internally / externally)?
   In what forms does it reach you (formal reports / briefings / email / phone / meetings etc)
   Is it pre-assessed by others first?

9. Do you, or the organisation, use any criteria or system to evaluate or grade the quality of information and intelligence gathered, shared or received?
   You
   FACT
   Internally sourced / developed intelligence
   Externally sourced / developed intelligence
   Can it be relied upon?

10. Is there anything more that you would like to add that we have not addressed?

[Closure – thank you for your time and participation]

Appendix Eighteen: Phase Two Interview Schedules

Various version of the semi-structured interview schedule were produced (listed in the order reproduced in this appendix):

- General interview schedule (used for most participants)
- Regulator interview schedule
- Government Strategy / Policy interview schedule
- Government Information Sharing Research Project interview schedule

Information and Intelligence Sharing in the Fight against Fraud

Interview Schedule [General]

This interview is being conducted as part of doctoral research into information and intelligence sharing in the fight against fraud. The aim of the research is to gain a view of the contemporary state of anti-fraud information and intelligence sharing, and to consider the problems impeding wider information sharing and how these may be overcome.

The interview is entirely voluntary, and your identity as a participant will not be disclosed in the final thesis, or in any other output detailing the findings of the research. This interview is being recorded – please could you confirm that you consent to it being recorded.

Section 1: Introductory

1. **Please could you provide a brief overview of your position and background as it relates to issues of fraud and information and intelligence sharing?**

2. **On a general basis, how do you think that organisations in the UK are performing in respect of sharing information for anti-fraud purposes?**

   Private Sector
   Public Sector
   Non-Profit Sector

3. **Do you think that any particular sectors or industries are particularly noteworthy for anti-fraud information sharing: either doing particularly well or badly?**

Section 2: Own Organisation's Model of Information and Intelligence Sharing

4. **Would you be able to provide me with an overview of how your organisation shares information and/or intelligence with others for the prevention or investigation of fraud?**

   With whom does it share?
   How does it share?
   What model does it use for information sharing?
   Does it work effectively?
   How is it organised?
   Information Sharing Agreements
   Conditions of use
   Data sharing standards / Protocols

Governance arrangements
Security

5. **Does your organisation, and/or your network, use any criteria or system to manage or grade the quality of information or intelligence shared or received (e.g. such as the National Intelligence Model, or 5x5x5)?**

6. **Does your organisation place any restrictions or conditions upon the information and intelligence shared with partners, and are you able to outline these?**

   Suspected/confirmed fraud
   How information/intelligence is used
   Onward sharing of information and intelligence (within or outside of network)

7. **How does your organisation manage and maintain its relationships with its information sharing partners?**

   Meetings
   Dedicated staff / points of contact
   Senior level relationships

Section 3: Political/Legal Barriers

8. **From your experience what have been the most significant political/legal challenges that have impeded, or that have had to be tackled in respect of, sharing anti-fraud information with other organisations?**

9. **How has your organisation overcome these challenges?**

10. **Do any political/legal barriers still exist that impede, or sometimes prevent, effective information or intelligence sharing with other organisations?**

11. **Are you aware of the forthcoming changes to the EU Directive on Data Protection?**

    If yes, how do you think that this may impact the environment for information and intelligence sharing in the UK?

Section 4: Organisational/Cultural Barriers

12. **From your experience what have been the most significant organisational and cultural challenges that have impeded, or that have had to be tackled in respect of, sharing anti-fraud information with other organisations?**

13. **How has your organisation overcome these challenges?**

14. **Has your organisation encountered issues relating to the human resistance to share information with partners, and how has it overcome such challenges?**

    Internal staff resistance
    External staff resistance

15. **How has your organisation and network approached issues of trust between information sharing partners?**

    Building Trust
    Tackling Lack of Trust

16. **Has your organisation had to deal with issues relating to organisational self interest impeding information sharing and, if so, how has it done so?**

    Selective or one-way sharing
    Failing to share despite agreements
    Seeking to dominate or control network/relationship/data

17. **From your organisation's experience, how do you see the role of senior level involvement and leadership in establishing and maintaining information sharing between multiple parties?**

18. **Have you had to deal with issues of information asymmetry (the imbalance of information held by different information sharing partners) impeding information sharing and, if so, how have these been dealt with?**

19. **Do any organisational / cultural barriers still exist that impede, or sometimes prevent, effective information or intelligence sharing with other organisations?**

Section 5: Technical Barriers

20. **From your/your organisation's experience what have been the most significant technical challenges that have impeded, or that have had to be tackled in respect of, sharing anti-fraud information with other organisations?**

21. **How has your organisation overcome these challenges?**

22. **Do any technical barriers still exist that impede, or sometimes prevent, effective information or intelligence sharing with other organisations?**

Section 6 – Final

23. **Is there anything that you would like to see done to better facilitate effective information and intelligence sharing in future in the UK?**

    Change to legislation
    System of licensing for those who hold and share data
    Training/accreditation

24. **In your view, what are the most important factors that help facilitate information sharing between organisations?**

25. **Is there anything more that you would like to add that we have not addressed?**

[Closure- thank participant for their time and assistance]

Information and Intelligence Sharing in the Fight against Fraud

Interview Schedule [Regulator]

This interview is being conducted as part of doctoral research into information and intelligence sharing in the fight against fraud. The aim of the research is to gain a view of the contemporary state of anti-fraud information and intelligence sharing, and to consider the problems impeding wider information sharing and how these may be overcome.

The interview is entirely voluntary, and your identity as a participant will not be disclosed in the final thesis, or in any other output detailing the findings of the research. This interview is being recorded – please could you confirm that you consent to it being recorded.

Section 1: Introductory

1. **Please could you provide a brief overview of your position and background in the organisation?**

2. **Does your position involve issues relating to information sharing between organisations?**

3. **Please could you provide me with an overview of the [ORG NAME] as an organisation?**
   Role
   Purview
   Where does it sit within Government / which Dept/Minister?
   How does it go about this work?

Section 2: Data Protection Act 1998

4. **Please could you provide me with an overview of the DPA in terms of its purpose and intent?**
   History
   Links to EU Directive
   Aims
   ICO Role in respect of DPA

5. **How does the DPA provide for data sharing for anti-fraud / anti-crime purposes?**
   Provisions
   Channels - inc. s.29(3)
   Rules

6. **From the [ORG NAME] perspective, how are the rules on data sharing interpreted and translated in the work that it does in this area?**
   Philosophy on sharing for anti-crime purposes?
   Encouragement
   Enforcement

7. **How do you perceive other organisations interpretation of DPA in respect of information sharing?**
   Barrier
   Misunderstood
   Hide Behind it
   Fear of Fines
   High Profile Breaches / Reputation Risk

   Public Sector
   Private Sector

8. **How can we best overcome some of the problems – especially cultural problems – in interpretation of DPA that prevent sharing?**
   Solutions
   Roles and Responsibilities

9. **Do you consider that the DPA in its current form provides sufficient channels to enable the effective sharing of information between organisations for combating fraud?**
   Why?
   Shortcomings
   Improvements
   Cross-Sector / Cross-Industry

10. **What safeguards are in place to protect privacy in respect of information sharing for prevention and detection of crime?**
    What types of protection?
    What enforcement?
    Why are these required?

11. **How does the DPA fit in with other legislation in the UK (and EU) in respect of information sharing?**
    General legislative environment
    Additional legislation (e.g. s.68 Serious Crime Act – SAFOs)
    Public Sector Gateways
    Departmental legislation (e.g. Customs & Excise Management Act)
        What takes precedent?

12. **How effective is the current legal infrastructure for enabling effective information sharing?**

13. **How do you see the current review of the EU Directive on Data Protection concluding – will there be a major change of direction?**
    Involvement of [ORG NAME]
    Anticipated outcomes
    Impact on UK Data Protection Legislation / Environment / Enforcement
    Impact on information sharing

14. **Aside from EU review, is there any additional work being conducted with a view to changes to DPA?**
    Current / Recent
    Planned
    Perceived need

Section 3: Need for Greater Data Sharing in UK for Anti-Fraud Purposes

15. **In respect of the widely perceived and acknowledged need for and role of information sharing to combat fraud, how do you perceive the role of the DPA within enabling this?**

16. **Does the DPA allow for large scale sharing of information for prevention purposes?**
    How is this achievable?
    What restrictions and controls?

17. **Does the DPA allow for small scale sharing of information for prevention & detection purposes?**
    How is this achievable?
    What restrictions and controls?

18. **What is the role of the [ORG NAME] in respect of information sharing for anti-fraud purposes?**
    Enabling / facilitating
    Regulating / enforcement
    How is it involved in work to facilitate information sharing?
    Involved in current Cabinet Office work?

19. **What is the role of the [ORG NAME] in respect of education of organisations with respect to information sharing issues?**
    What does it do?
    How does it do it?
    Public Sector
    Private Sector
    Is the work effective in improving information sharing practice?

[C. Watson Interview Schedule – Final (Post-Pilot)]

20. **What guidance/support do you currently provide to organisations seeking to share information for anti-fraud purposes?**
    Who is it for?
    What purpose?
    Is it effective?

21. **How does the [ORG NAME] work with organisations involved in, or wanting to be involved in, the sharing of data for anti-fraud purposes?**
    Consultation
    Guidance
    Audit
    Regulation

22. **Do you perceive there to be a consistent balance at present in the competing political appetites for greater information sharing and protection of privacy?**
    Can an effective balance be struck for the greatest good?
    Has the balance been struck?
    How can we improve this?

Section 4: Scenarios

23. **If *Organisation A* wanted to seek specific information from *Organisation B* on an ad-hoc basis in relation to suspected fraud, how can (or should) it goes about this in a way that would be consistent with the DPA?**

24. **If *Organisation A* wanted to share data in bulk on a regular basis with *Organisation B* for the prevention or detection of fraud, how can (or should) it goes about this in a way that would be consistent with the DPA?**

Section 7: Final

25. **Is there anything that you would like to see done to better facilitate effective information and intelligence sharing in future in the UK?**

26. **What, in your view, are the most important factors that may help facilitate effective information sharing for anti-fraud purposes?**

27. **Are you aware of any examples of good practice or innovation in this area, in the UK or overseas, that could be utilised more widely in the UK?**

28. **Is there anything more that you would like to add that we have not addressed?**

[Closure- thank participant for their time and assistance]

Information and Intelligence Sharing in the Fight against Fraud

Interview Schedule [Government Strategic / Policy]

This interview is being conducted as part of doctoral research into information and intelligence sharing in the fight against fraud. The aim of the research is to gain a view of the contemporary state of anti-fraud information and intelligence sharing, and to consider the problems impeding wider information sharing and how these may be overcome.

The interview is entirely voluntary, and your identity as a participant will not be disclosed in the final thesis, or in any other output detailing the findings of the research. This interview is being recorded – please could you confirm that you consent to it being recorded.

Section 1: Introductory

1. **Please could you provide a brief overview of your position and background as it relates to issues of fraud and information and intelligence sharing?**

2. **On a general basis, how do you think that organisations in the UK are performing in respect of sharing information for anti-fraud purposes?**

   Private Sector
   Public Sector
   Non-Profit Sector

3. **Do you think that any particular sectors or industries are particularly noteworthy for anti-fraud information sharing: either doing particularly well or badly?**

Section 2: Own Organisation's Involvement in Information and Intelligence Sharing

4. **Would you be able to provide me with an overview of how your organisation is involved in issues of sharing information and/or intelligence with others?**

   What are the aims?
   Why are they the aims?
   Who is involved?
   How is this conducted?
   What are the outcomes/intended outcomes?
   How is the work progressing?
   Is it successful?
   Why / Why not?

5. **What issues do you find arising from the work that impede collaboration between organisations?**

   Co-operation
   Willingness to engage in process
   Are the right organisations involved?
   Are the right people within those organisations involved (Committed, Decision Makers)?
   Problems cited by parties engaged in process

Section 3: Legal Channels and Infrastructure

6. **How effective do you see the current legal infrastructure in terms of providing appropriate legal channels for information sharing?**

7. **How do you perceive the role of the Data Protection Act in enabling information sharing?**

   Does it provide appropriate channels?
   Are the channels open to most organisations?
   Do you see any problems caused by the interpretation of the DPA?
   Do you think that the DPA is in need of reform?
   Has the government/your office discussed these issues with the Information Commissioner?

8. **Are you aware of the forthcoming changes to the EU Directive on Data Protection?**

   If yes, how do you think that this may impact the environment for information and intelligence sharing in the UK?

9. **How do you perceive the role of the channel established by s.68 of the Serious Crime Act allowing public sector bodies to share with Specified Anti-Fraud Organisations?**

   Has it made a difference?
   Is it working as intended?
   Why / Why not?
   Are there many SAFOs?
   Are public sector organisations sharing information with the SAFOs?

10. **How do you perceive the role of the current legal gateways between departments allowing sharing in specific circumstances?**

    Do they work effectively?
    Are they far reaching enough?
    Are more channels / more general channels / needed?

11. **Do you think that additional legislation, or changes to existing legislation, is needed to improve the practice of information sharing?**

    Public to public sector?
    Public to private sector?
    What changes would be helpful?
    Specific versus general legislation and powers?
    Is there an appetite in government to consider legislative reform?

Section 4: Political/Legal Issues

12. **From your experience what have been the most significant political/legal challenges that have impeded, or that have had to be tackled in respect of, sharing anti-fraud information with other organisations?**

13. **How have you approached these challenges when they've arisen?**

14. **Do any political/legal barriers still exist that impede, or sometimes prevent, effective information or intelligence sharing with other organisations?**

Section 5: Organisational/Cultural Barriers

15. **From your experience what have been the most significant organisational and cultural challenges that have had to be tackled in respect of, sharing anti-fraud information?**

16. **How have you approached these challenges?**

17. **Have you encountered issues relating to the human resistance to share information with partners, and how has it overcome such challenges?**

    Internal staff resistance
    External staff resistance

18. **How have you approached issues of trust between information sharing partners?**

    Building Trust
    Tackling Lack of Trust

19. **Have you had to deal with issues relating to organisational self interest impeding information sharing?**

    Selective or one-way sharing

[C. Watson Interview Schedule – Final (Post-Pilot)]

Failing to share despite agreements
Seeking to dominate or control network/relationship/data

20. **From your experience, how do you see the role of senior level involvement and leadership in establishing and maintaining information sharing between multiple parties?**

21. **Have you had to deal with issues of information asymmetry (the imbalance of information held by different information sharing partners) impeding information sharing and, if so, how have these been dealt with?**

22. **Do any organisational / cultural barriers still exist that impede, or sometimes prevent, effective information or intelligence sharing with other organisations?**

Section 6: Technical Barriers

23. **From your experience what have been the most significant technical challenges that have had to be tackled in respect of sharing anti-fraud information?**

24. **How have you approached these challenges?**

25. **Do any technical barriers still exist that impede, or sometimes prevent, effective information or intelligence sharing with other organisations?**

Section 7: Final

26. **Is there anything that you would like to see done to better facilitate effective information and intelligence sharing in future in the UK?**

    Change to legislation
    System of licensing for those who hold and share data
    Training/accreditation

27. **Are you aware of any good practice or innovation in this area, in the UK or overseas, that could be utilised more widely in the UK?**

28. **Is there anything more that you would like to add that we have not addressed?**

[Closure- thank participant for their time and assistance]

[C. Watson Interview Schedule – Final (Post-Pilot)]

Information and Intelligence Sharing in the Fight against Fraud

Interview Schedule [Government Information Sharing Research Project]

This interview is being conducted as part of doctoral research into information and intelligence sharing in the fight against fraud. The aim of the research is to gain a view of the contemporary state of anti-fraud information and intelligence sharing, and to consider the problems impeding wider information sharing and how these may be overcome.

The interview is entirely voluntary, and your identity as a participant will not be disclosed in the final thesis, or in any other output detailing the findings of the research. This interview is being recorded – please could you confirm that you consent to it being recorded.

Section 1: Introductory

1. **Please could you provide a brief overview of your position and background as it relates to issues of fraud and information and intelligence sharing?**

2. **On a general basis, how do you think that organisations in the UK are performing in respect of sharing information for anti-fraud purposes?**

   Private Sector
   Public Sector
   Non-Profit Sector

3. **Do you think that any particular sectors or industries are particularly noteworthy for anti-fraud information sharing: either doing particularly well or badly?**

4. **Please could you give me an overview of the work that you have been doing with the Home Office to map fraud flows?**

5. **What has been done?**

6. **Why has it been done?**

7. **What was the scope of the work?**

8. **How have you done the mapping?**

9. **Over what timeframe has the work been undertaken?**

10. **What was the extent of the mapping?**

[C. Watson Interview Schedule – Final (Post-Pilot)]

UK / Overseas
Sectors
Comprehensiveness, etc?

11. **Have there been any problems in compiling it?**

12. **Are there any gaps in the coverage that you're aware of?**

13. **What is/will be the end product?**

    What will it look like?
    How will it be used?
    Who will have access to it?
    How will it be kept up to date?

14. **How does this fit into the wider work that the Home Office is doing in this area?**

15. **What has the work shown so far in terms of the picture of information sharing?**

    Findings
    Effectiveness
    Extent
    Other lessons

Section 2: Own Organisation's Model of Information and Intelligence Sharing

16. **Would you be able to provide me with an overview of how your organisation shares information and/or intelligence with others for the prevention or investigation of fraud?**

    With whom does it share?
    How does it share?
    What model does it use for information sharing?
    Does it work effectively?
    How is it organised?
    Information Sharing Agreements
    Conditions of use
    Data sharing standards / Protocols
    Governance arrangements
    Security

17. **Does your organisation, and/or your network, use any criteria or system to manage or grade the quality of information or intelligence shared or received (e.g. such as the National Intelligence Model, or 5x5x5)?**

18. **Does your organisation place any restrictions or conditions upon the information and intelligence shared with partners, and are you able to outline these?**

    Suspected/confirmed fraud
    How information/intelligence is used
    Onward sharing of information and intelligence (within or outside of network)

19. **How does your organisation manage and maintain its relationships with its information sharing partners?**

    Meetings
    Dedicated staff / points of contact
    Senior level relationships

Section 3: Political/Legal Barriers

20. **From your experience what have been the most significant political/legal challenges that have impeded, or that have had to be tackled in respect of, sharing anti-fraud information with other organisations?**

21. **How has your organisation overcome these challenges?**

22. **Do any political/legal barriers still exist that impede, or sometimes prevent, effective information or intelligence sharing with other organisations?**

23. **Are you aware of the forthcoming changes to the EU Directive on Data Protection?**

    If yes, how do you think that this may impact the environment for information and intelligence sharing in the UK?

Section 4: Organisational/Cultural Barriers

24. **From your experience what have been the most significant organisational and cultural challenges that have impeded, or that have had to be tackled in respect of, sharing anti-fraud information with other organisations?**

25. **How has your organisation overcome these challenges?**

[C. Watson Interview Schedule – Final (Post-Pilot)]

26. **Has your organisation encountered issues relating to the human resistance to share information with partners, and how has it overcome such challenges?**

    Internal staff resistance
    External staff resistance

27. **How has your organisation and network approached issues of trust between information sharing partners?**

    Building Trust
    Tackling Lack of Trust

28. **Has your organisation had to deal with issues relating to organisational self interest impeding information sharing and, if so, how has it done so?**

    Selective or one-way sharing
    Failing to share despite agreements
    Seeking to dominate or control network/relationship/data

29. **From your organisation's experience, how do you see the role of senior level involvement and leadership in establishing and maintaining information sharing between multiple parties?**

30. **Have you had to deal with issues of information asymmetry (the imbalance of information held by different information sharing partners) impeding information sharing and, if so, how have these been dealt with?**

31. **Do any organisational / cultural barriers still exist that impede, or sometimes prevent, effective information or intelligence sharing with other organisations?**

Section 5: Technical Barriers

32. **From your/your organisation's experience what have been the most significant technical challenges that have impeded, or that have had to be tackled in respect of, sharing anti-fraud information with other organisations?**

33. **How has your organisation overcome these challenges?**

34. **Do any technical barriers still exist that impede, or sometimes prevent, effective information or intelligence sharing with other organisations?**

[C. Watson Interview Schedule – Final (Post-Pilot)]

Section 6 – Final

35. **Is there anything that you would like to see done to better facilitate effective information and intelligence sharing in future in the UK?**

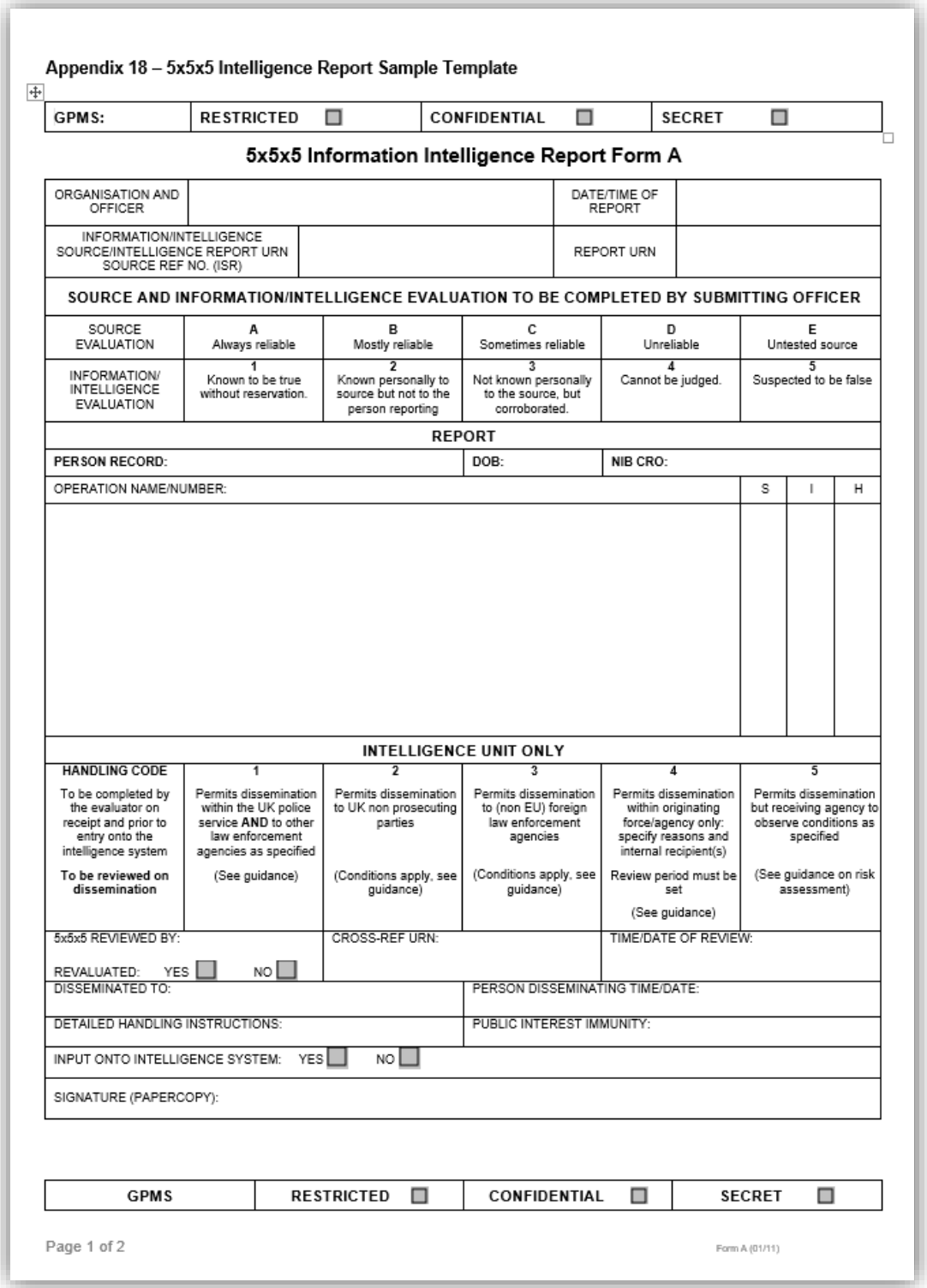
    Change to legislation
    System of licensing for those who hold and share data
    Training/accreditation

36. **In your view, what are the most important factors that help facilitate information sharing between organisations?**

37. **Is there anything more that you would like to add that we have not addressed?**

[Closure- thank participant for their time and assistance]

Appendix Nineteen: 5x5x5 Information/Intelligence Report Template



Appendix 18 – 5x5x5 Intelligence Report Sample Template

GPMS:	RESTRICTED ☐	CONFIDENTIAL ☐	SECRET ☐

5x5x5 Information Intelligence Report Form A

ORGANISATION AND OFFICER		DATE/TIME OF REPORT	
INFORMATION/INTELLIGENCE SOURCE/INTELLIGENCE REPORT URN SOURCE REF NO. (ISR)		REPORT URN	

SOURCE AND INFORMATION/INTELLIGENCE EVALUATION TO BE COMPLETED BY SUBMITTING OFFICER

SOURCE EVALUATION	A Always reliable	B Mostly reliable	C Sometimes reliable	D Unreliable	E Untested source
INFORMATION/ INTELLIGENCE EVALUATION	1 Known to be true without reservation.	2 Known personally to source but not to the person reporting	3 Not known personally to the source, but corroborated.	4 Cannot be judged.	5 Suspected to be false

REPORT

PERSON RECORD:	DOB:	NIB CRO:			
OPERATION NAME/NUMBER:			S	I	H

INTELLIGENCE UNIT ONLY

HANDLING CODE To be completed by the evaluator on receipt and prior to entry onto the intelligence system **To be reviewed on dissemination**	1 Permits dissemination within the UK police service **AND** to other law enforcement agencies as specified (See guidance)	2 Permits dissemination to UK non prosecuting parties (Conditions apply, see guidance)	3 Permits dissemination to (non EU) foreign law enforcement agencies (Conditions apply, see guidance)	4 Permits dissemination within originating force/agency only: specify reasons and internal recipient(s) Review period must be set (See guidance)	5 Permits dissemination but receiving agency to observe conditions as specified (See guidance on risk assessment)

5x5x5 REVIEWED BY: REVALUATED: YES ☐ NO ☐	CROSS-REF URN:	TIME/DATE OF REVIEW:
DISSEMINATED TO:	PERSON DISSEMINATING TIME/DATE:	
DETAILED HANDLING INSTRUCTIONS:	PUBLIC INTEREST IMMUNITY:	
INPUT ONTO INTELLIGENCE SYSTEM: YES ☐ NO ☐		
SIGNATURE (PAPERCOPY):		

GPMS	RESTRICTED ☐	CONFIDENTIAL ☐	SECRET ☐

Page 1 of 2

Form A (01/11)

5x5x5 Continuation Form B

INFORMATION/INTELLIGENCE SOURCE/INTELLIGENCE REPORT URN SOURCE REF NO. (ISR)		REPORT URN	

REPORT		
NOMINAL:	**DOB:**	**NIB CRO:**

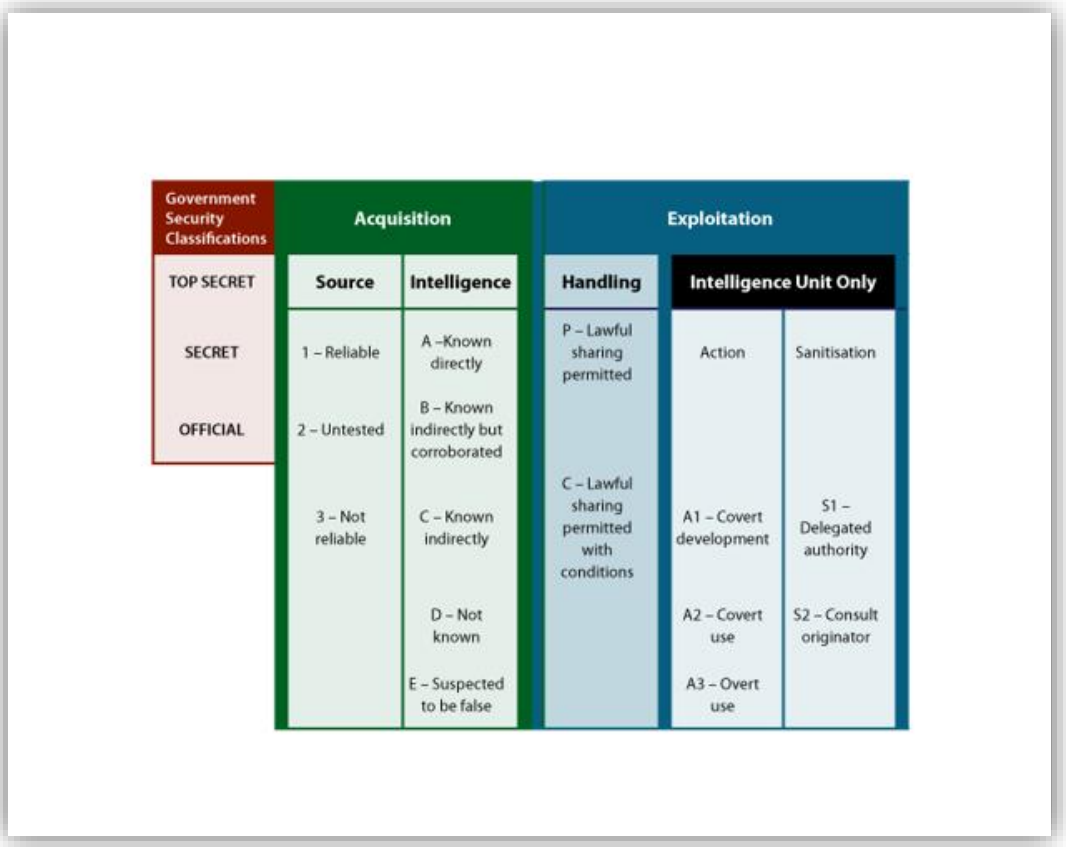
OPERATION NAME/NUMBER:	S	I	H

Page 2 of 2

Form A (01/11)

Source: Manchester Safeguarding Children Board: www.manchesterscb.org.uk/displaydoc.asp?id=466

Appendix Twenty: 3x5x2 Information/Intelligence Report Grading System



Government Security Classifications	Acquisition		Exploitation		
	Source	Intelligence	Handling	Intelligence Unit Only	
TOP SECRET	1 – Reliable	A –Known directly	P – Lawful sharing permitted	Action	Sanitisation
SECRET	2 – Untested	B – Known indirectly but corroborated	C – Lawful sharing permitted with conditions	A1 – Covert development	S1 – Delegated authority
OFFICIAL	3 – Not reliable	C – Known indirectly		A2 – Covert use	S2 – Consult originator
		D – Not known		A3 – Overt use	
		E – Suspected to be false			

Source: College of Policing: https://www.app.college.police.uk/app-content/intelligence-management/intelligence-report/